

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-289297

(43)Date of publication of application : 10.10.2003

(51)Int.Cl.

H04L 9/08

(21)Application number : 2003-014027

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing :

22.01.2003

(72)Inventor : MATSUZAKI NATSUME  
NAKANO TOSHIHISA  
MATSUMOTO TSUTOMU

(30)Priority

Priority number : 2002016547

Priority date : 25.01.2002

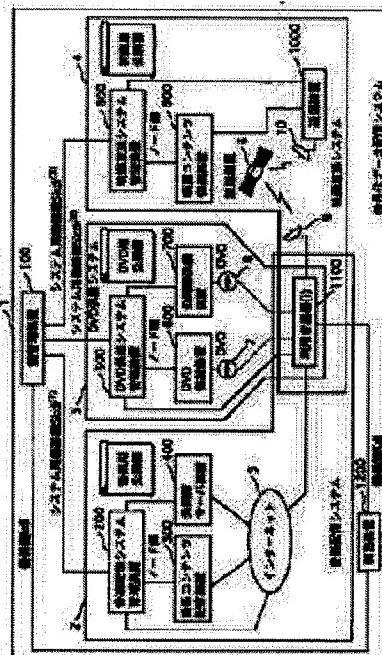
Priority country : JP

## (54) DATA DISTRIBUTION SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To enable each of content supply system to use a group key management method employing flexible and unique structures, when a single user apparatus is connected a plurality of content supply systems.

**SOLUTION:** A manager of each content supply system uses a system apparatus key, distributed from a key management organization to generate a public list corresponding to a unique tree structure, and discloses the list, when the content supply system is constructed. The user apparatus stores only the apparatus key, corresponding to a leaf of the tree structure. Using the public list which is disclosed via a web site or package media, the user apparatus constructs the tree structure sequentially from the bottom to the top, and derives a node key corresponding to the user apparatus. Next, the user apparatus decrypts an encrypted content by using the node key.



(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-289297

(P2003-289297A)

(43)公開日 平成15年10月10日(2003.10.10)

(51)Int.Cl.<sup>7</sup>

H 04 L 9/08

識別記号

F I

テ-マコード(参考)

H 04 L 9/00

6 0 1 B 5 J 1 0 4

6 0 1 E

6 0 1 A

審査請求 未請求 請求項の数40 OL (全 58 頁)

(21)出願番号	特願2003-14027(P2003-14027)	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成15年1月22日(2003.1.22)	(72)発明者	松崎 なつめ 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(31)優先権主張番号	特願2002-16547(P2002-16547)	(72)発明者	中野 稔久 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(32)優先日	平成14年1月25日(2002.1.25)	(74)代理人	100090446 弁理士 中島 司朗
(33)優先権主張国	日本 (JP)		

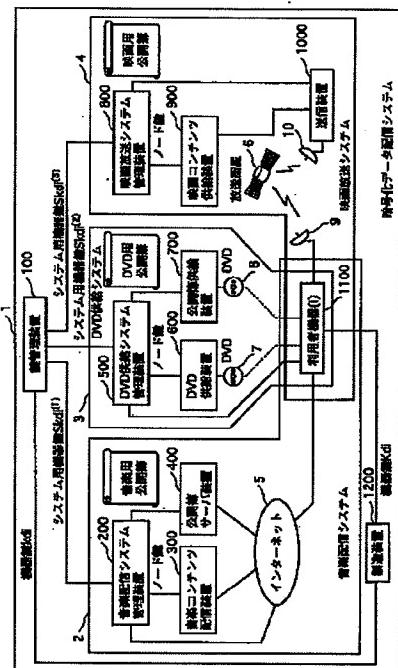
最終頁に続く

### (54)【発明の名称】 データ配信システム

#### (57)【要約】

【課題】1個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の木構造を用いたグループ鍵管理方法を使用することできるようとする。

【解決手段】コンテンツ供給システムの管理者は、鍵管理機関より配布されたシステム用の機器鍵を用いて、独自の木構造に対応する公開簿を生成し、システム構築時に公開する。利用者機器は、木構造のリーフに対応した機器鍵だけを保持する。Webページやパッケージメディアを介して公開された公開簿を用いて、利用者機器は、下から上に順次木構造を構築し、対応するノード鍵を求める。次に、ノード鍵を用いて暗号化コンテンツを復号する。



## 【特許請求の範囲】

【請求項1】 鍵管理装置と複数のコンテンツ供給装置と1個以上の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、各利用者機器は、暗号化コンテンツを復号して利用し、

各利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、

それぞれ、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力する複数のコンテンツ供給装置と、

それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成し、生成した前記第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する1個以上の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項2】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、

それぞれ、前記第1システム用機器鍵を受け取り、前記第1システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開する複数のコンテンツ供給装置と、

それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開簿を取得し、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報

に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成し、前記第2システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する1個の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項3】 前記コンテンツ供給装置は、前記第1システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、

前記利用者機器は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定することを特徴とする請求項2に記載のデータ配信システム。

【請求項4】 前記コンテンツ供給装置は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、公開し、

前記利用者機器は、Webサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得することを特徴とする請求項3に記載のデータ配信システム。

【請求項5】 前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する情報のみを出し、前記利用者機器は、前記公開簿のうち、前記利用者機器に関連する情報のみを取得することを特徴とする請求項4に記載のデータ配信システム。

【請求項6】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおいて、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵出力手段と、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した第1システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成手段とを備えることを特徴とする鍵管理装置。

【請求項7】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、

デジタル著作物であるコンテンツを記憶している記憶手段と、

前記鍵管理装置から前記第1システム用機器鍵を取得する取得手段と、

前記第1システム用機器鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備えることを特徴とするコンテンツ供給装置。

**【請求項8】** 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している記憶手段と、

前記鍵管理装置から前記第1システム用機器鍵を取得する取得手段と、

前記第1システム用機器鍵に基づいて、コンテンツを暗号化する際にに基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、

前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成する公開簿生成手段と、生成した前記公開簿を公開し、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備えることを特徴とするコンテンツ供給装置。

**【請求項9】** 前記出力手段は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、公開することを特徴とする請求項8に記載のコンテンツ供給装置。

**【請求項10】** 前記公開簿生成手段は、前記公開簿のうち、前記利用者機器に関する利用者機器関連情報を生成し、

前記出力手段は、前記利用者機器関連情報を、公開することを特徴とする請求項9に記載のコンテンツ供給装置。

**【請求項11】** 前記暗号手段は、前記第1システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定することを特徴とする請求項8に記載のコンテンツ供給装置。

**【請求項12】** 前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てら

れたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成することを特徴とする請求項11に記載のコンテンツ供給装置。

**【請求項13】** 前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、(a) 当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、(b) 当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、(c) 生成した暗号化ノード鍵を含む前記公開簿を生成することを特徴とする請求項11に記載のコンテンツ供給装置。

**【請求項14】** kを2以上の整数とし、mを0以上の整数とし、前記木構造をk分木とし、各ノード鍵を(x, y)平面上の点とみなし、

前記公開簿生成手段は、(x, y)平面上において、共通の親ノードを持つk個の全てのノードのノード鍵を結ぶ(k+m-1)次の曲線を生成し、前記曲線上のノード鍵以外の(k+m-1)個の点を含む前記公開簿を生成することを特徴とする請求項11に記載のコンテンツ供給装置。

**【請求項15】** 前記公開簿生成手段は、前記(k+m-1)次の曲線から一方向性関数を用いて予め決められた手法により一意に定まる点を、共通の親ノードに対応するノード鍵とすることを特徴とする請求項14に記載のコンテンツ供給装置。

**【請求項16】** 前記公開簿生成手段は、(a) 公開鍵暗号の秘密鍵と公開鍵のペアを生成し、(b) 生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、(c) 前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、

前記出力手段は、前記公開簿を公開することを特徴とする請求項11に記載のコンテンツ供給装置。

**【請求項17】** 前記公開簿生成手段は、(a) 素数pとqの積nを計算し、(b) p-1とq-1の最小公倍数Lを求め、(c) nと互いに素となるL以下の任意の整数eを求め、(d) Lを法とするeの逆元d

を求めてこれを秘密鍵とし、(e) 前記整数e及び前記積nを含む前記公開簿を生成し、(f) 前記ノードに対応するノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス情報との排他的論理和を求め、(g) 排他的論理和を、前記秘密鍵dを用いて暗号化して暗号化ノード鍵を生成し、(h) 生成した暗号化ノード鍵を当該パスに接続する子ノードに対応するノード鍵とすることを特徴とする請求項16に記載のコンテンツ供給装置。

【請求項18】 前記公開簿生成手段は、

(A) 木構造のリーフとそのすぐ上位のノードの間に関しては、

(a) 前記木構造のリーフのすぐ上位の各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は (b) 木構造のリーフのすぐ上位の各ノードについて、当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は (c)  $k$  を2以上の整数とし、 $m$  を0以上の整数とし、前記木構造を  $k$  分木とし、各ノード鍵を  $(x, y)$  平面上の点とみなし、 $(x, y)$  平面上において、共通の親ノードを持つ  $k$  個の全てのリーフのノード鍵を結ぶ  $(k+m-1)$  次の曲線を生成し、前記曲線上のノード鍵以外の  $(k+m-1)$  個の点を含む前記公開簿を生成し、

(B) 上記以外のノードの間に関しては、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、前記木構造のリーフ及びすぐ上位のノードを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とすることを特徴とする請求項11に記載のコンテンツ供給装置。

【請求項19】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、前記鍵管理装置から前記機器鍵を受け取る取得手段と、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信手段と、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム

用機器鍵生成手段と、

生成した第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備えることを特徴とする利用者機器。

【請求項20】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報を基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、前記第1システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開し、前記鍵管理装置から前記機器鍵を受け取り、公開された前記公開簿を取得し、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る取得手段と、

前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成手段と、

前記第2システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定するデバイス鍵特定手段と、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備えることを特徴とする利用者機器。

【請求項21】 前記コンテンツ供給装置は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、公開し、前記取得手段は、Webサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得することを特徴とする請求項20に記載の利用者機器。

【請求項22】 前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成して公開し、前記取得手段は、前記利用者機器関連情報を取得し、前記デバイス鍵特定手段は、取得した前記利用者機器関連情報から当該利用者機器に対応する前記デバイス鍵を特定することを特徴とする請求項21に記載の利用者機器。

【請求項23】 前記コンテンツ供給装置は、前記第1システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造

を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定することを特徴とする請求項20に記載の利用者機器。

【請求項24】 前記デバイス鍵特定手段は、取得した前記公開簿を用いて、前記木構造において、あるリーフに割り当てられた第2システム用機器鍵から、当該リーフからルートに至る経路上の各ノードに対応するノード鍵を順次求めることを特徴とする請求項23に記載の利用者機器。

【請求項25】 前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を用いて、取得した前記公開簿内の暗号化ノード鍵を復号して、当該ノードの親ノードのノード鍵を求めることが特徴とする請求項24に記載の利用者機器。

【請求項26】 前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、(a) 当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、(b) 当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、(c) 生成した暗号化ノード鍵を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該ノードに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該ノードの親ノードのノード鍵として求めることを特徴とする請求項24に記載の利用者機器。

【請求項27】  $k$  を2以上の整数とし、 $m$  を0以上の整数とし、前記木構造を  $k$  分木とし、各ノード鍵を  $(x, y)$  平面上の点とみなし、

前記コンテンツ供給装置は、 $(x, y)$  平面上において、共通の親ノードを持つ  $k$  個の全てのノードのノード鍵を結ぶ  $(k+m-1)$  次の曲線を生成し、前記曲線上のノード鍵以外の  $(k+m-1)$  個の点を含む前記公開簿を生成し、

前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵と、公開された公開簿内の  $(k+m-1)$  個の点とを結ぶ、 $(k+m-1)$  次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該ノード

の親ノードに対応するノード鍵を求めることが特徴とする請求項24に記載の利用者機器。

【請求項28】 前記コンテンツ供給装置は、(a) 公開鍵暗号の秘密鍵と公開鍵のペアを生成し、(b) 生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、(c) 前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、(d) 前記公開簿を公開し、

前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とすることを特徴とする請求項24に記載の利用者機器。

【請求項29】 前記コンテンツ供給装置は、(a) 秘密の素数  $p$  と  $q$  の積  $n$  を計算し、(b)  $p-1$  と  $q-1$  の最小公倍数  $L$  を求め、(c)  $n$  と互いに素となる  $L$  以下の任意の整数  $e$  を求め、(d)  $L$  を法とする  $e$  の逆元  $d$  を求めてこれを秘密鍵とし、(e) 前記整数  $e$  及び前記積  $n$  を含む前記公開簿を生成し、(f) 前記ノードに対応するノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス情報との排他的論理和を求め、(g) 排他的論理和を、前記秘密鍵  $d$  を用いて暗号化して暗号化ノード鍵を生成し、

(h) 生成した暗号化ノード鍵を当該パスに接続する子ノードに対応するノード鍵し、

前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を、公開された公開簿内の公開鍵  $(e, n)$  を用いて復号し、その結果と、当該ノードの親ノードに接続するパスのパス情報をとの排他的論理和を求め、得られた排他的論理和を、当該ノードの親ノードに対応したノード鍵とすることを特徴とする請求項28に記載の利用者機器。

【請求項30】 前記コンテンツ供給装置は、  
(A) 木構造のリーフとそのすぐ上位のノードの間に関しては、

(a) 前記木構造のリーフのすぐ上位の各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は(b) 木構造のリーフのすぐ上位の各ノードについて、当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、又は(c)  $k$  を2以上の整数とし、 $m$  を0以上の整

数とし、前記木構造を  $k$  分木とし、各ノード鍵を  $(x, y)$  平面上の点とみなし、 $(x, y)$  平面上において、共通の親ノードを持つ  $k$  個の全てのリーフのノード鍵を結ぶ  $(k+m-1)$  次の曲線を生成し、前記曲線上のノード鍵以外の  $(k+m-1)$  個の点を含む前記公開簿を生成し、

(B) 上記以外のノードの間に関しては、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、前記木構造のリーフ及びすぐ上位のノードを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、前記デバイス鍵特定手段は、

(A) 木構造のリーフとそのすぐ上位のノードの間に関しては、

(a) 前記木構造の 1 個のリーフに対応するノード鍵を用いて、公開された公開簿内の暗号化ノード鍵を復号して、当該リーフの親ノードのノード鍵を求め、

(b) 前記木構造の 1 個のリーフに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該リーフに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該リーフの親ノードのノード鍵として求め、又は (c) 前記木構造の 1 個のリーフに対応するノード鍵と、公開された公開簿内の  $(k+m-1)$  個の点とを結ぶ、 $(k+m-1)$  次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該リーフの親ノードに対応するノード鍵を求め、

(B) 上記以外のノードの間に関しては、前記木構造のリーフ及びすぐ上位のノードを除くノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とすることを特徴とする請求項 24 に記載の利用者機器。

【請求項 31】 鍵管理装置と複数のシステム管理装置と前記同数のコンテンツ送出装置と 1 個の利用者機器とから構成されるデータ配信システムであって、各システム管理装置は、各コンテンツ送出装置に対応しており、各コンテンツ送出装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各システム管理装置について、前記機器鍵及び当該システム管理装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第 1 システム用機器鍵を生成し、生成した前記第 1 システム用機器鍵を当該システム管理装置へ出力する鍵管理装置と、それぞれ、前記第 1 システム用機器鍵を受け取り、前記

第 1 システム用機器鍵に基づいて、コンテンツを暗号化する際にに基づくデバイス鍵を決定し、決定した前記デバイス鍵を対応する前記コンテンツ送出装置へ出力し、前記第 1 システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開する複数のシステム管理装置と、

それぞれ、前記デバイス鍵を受け取り、受け取った前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力する複数のコンテンツ送出装置と、

前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開簿を取得し、前記機器鍵及び前記システム管理装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第 2 システム用機器鍵を生成し、前記第 2 システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する 1 個の利用者機器とから構成されることを特徴とするデータ配信システム。

【請求項 32】 鍵管理装置で用いられる鍵管理方法であって、鍵管理装置と複数のコンテンツ供給装置と 1 個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第 1 システム用機器鍵を生成し、生成した第 1 システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とする鍵管理方法。

【請求項 33】 鍵管理装置で用いられる鍵管理用のコンピュータプログラムであって、鍵管理装置と複数のコンテンツ供給装置と 1 個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第 1 システム用機器鍵を生成し、生成した第 1 システム用機器鍵を前

記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とするコンピュータプログラム。

【請求項34】 鍵管理装置で用いられる鍵管理用のコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記鍵管理装置は、前記利用者機器へ前記利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、

前記コンピュータプログラムは、

前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵生成ステップと、

各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した第1システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成ステップとを含むことを特徴とする記録媒体。

【請求項35】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給方法であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、デジタル著作物であるコンテンツを記憶している記憶手段を含み、

前記鍵管理装置から前記第1システム用機器鍵を取得する取得ステップと、

前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とするコンテンツ供給方法。

【請求項36】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給用のコンピュータプログラムであって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1

1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、デジタル著作物であるコンテンツを記憶している記憶手段を含み、

前記鍵管理装置から前記第1システム用機器鍵を取得する取得ステップと、

前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とするコンピュータプログラム。

【請求項37】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置で用いられるコンテンツ供給用のコンピュータプログラムを記録している記録媒体であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、デジタル著作物であるコンテンツを記憶している記憶手段を含み、

前記コンピュータプログラムは、

前記鍵管理装置から前記第1システム用機器鍵を取得する取得ステップと、

前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成する暗号ステップと、

生成した前記暗号化コンテンツを利用者機器へ出力する出力ステップとを含むことを特徴とする記録媒体。

【請求項38】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられる方法であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力し、

前記鍵管理装置から前記機器鍵を受け取る取得ステップと、

前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、

前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性閾数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成ステップと、生成した第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とする方法。

【請求項39】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられるコンピュータプログラムであって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性閾数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出し、前記鍵管理装置から前記機器鍵を受け取る取得ステップと、

前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性閾数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成ステップと、生成した第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とするコンピュータプログラム。

【請求項40】 鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性閾数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出し、前記コンピュータプログラムは、前記鍵管理装置から前記機器鍵を受け取る取得ステップ

と、

前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信ステップと、

前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性閾数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成ステップと、生成した第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップとを含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データを暗号化して配信する技術に関する。

【0002】

【従来の技術】 近年、映画や音楽などのデジタルコンテンツを、DVD (Digital VersatileDisk) などのパッケージメディアや放送、通信を用いて、特定の機器に配信するビジネスが広がっている。このようなビジネスにおいて、コンテンツの著作権を保護するために、コンテンツは、暗号化されて特定の機器に配信される。特定の機器は、著作権者との合意による制限の下でのみ、予め機器に埋め込まれている機器鍵を用いて暗号化コンテンツを復号し、コンテンツの再生や複製を行う。

【0003】 大容量のコンテンツを配信する場合には、1個のグループ鍵を用いてコンテンツが暗号化され、さらにグループ鍵が特定の機器だけに共有できるよう暗号化されるという2段階の暗号方法を探るのが一般的である。本明細書では、このように個別の機器鍵を用いて1個のグループ鍵を共有する方法を、グループ鍵管理方法と呼ぶことにする。

【0004】 最も自明なグループ鍵管理方法では、コンテンツ供給者は、グループ鍵を各機器が備える機器鍵を用いて暗号化して暗号化鍵情報を生成し、この暗号化鍵情報を暗号化コンテンツと対応させて配信する。指定された機器は、暗号化鍵情報より自身の機器鍵を用いてグループ鍵を算出し、このグループ鍵を用いて暗号化コンテンツを復号する。しかしながら、自明な方法ではグループの構成メンバーが多い場合、暗号化鍵情報のデータ量が多くなる。そこで、如何にこのデータ量を削減して効率的にグループ鍵を配信するかに関して、多くの研究がなされている。

【0005】 中でも、各機器が複数の機器鍵を保持し、その共有関係を木構造で表現する木構造鍵管理方法は、インターネット上の新技術の標準化を検討しているIETF (The Internet Engineering Task Force)において盛んに議論されており、多くの研究成果が発表されている。木構造鍵管理方法において、基本的には木構造の各節はノードと呼ばれ、最下位のノードであるリーフに個々の機器が割り当てられる。各機器は、リーフから、

最上位のノードであるルートまでの経路上に存在するノードに対応するノード鍵を保管する。なお、ノードとノードを結ぶ経路をパスと呼ぶ。鍵管理者は、複数の機器が共通に保持するノード鍵を用いてグループ鍵を暗号化することにより、暗号化鍵情報を削減する。

【0006】このような鍵管理方法が盛んに研究されている理由として、鍵管理者が新しい機器をグループに追加する場合や、何らかの理由で特定の機器をグループから排除する場合にも、情報量が少ない暗号化鍵情報によりグループ鍵を配布できること、あるノードをルートとした部分木を、現実の組織に対応させることにより、組織単位での追加や排除も可能であることなどが挙げられる。

【0007】木構造を用いたグループ鍵管理方法を、代表的な木構造分割方法を例にして説明する。詳細は、非特許文献1に詳しく述べられている。

【非特許文献1】「デジタルコンテンツ保護用鍵管理方式 (Key management system for digital content protection)」(中野稔久、大森基司、館林誠著、2001年暗号と情報セキュリティシンポジウム講演論文集、A5-5、2001—SCIS 2001, The 2001 Symposium on Cryptography and Information Security0iso, Japan, January 23-26, 2001. The Institute of Electronics, Information and Communication Engineers)

【0008】非特許文献1により開示されている木構造分割方法では、各機器は、それぞれ木のリーフに配置され、リーフからルートに至るすべてのノードに対応したノード鍵を保持する。図54に示すように、機器1は、機器固有の鍵k<sub>d1</sub>及びKeyD、KeyB、KeyAを保持している。KeyDは、機器1、2の共有鍵であり、KeyBは、機器1～4の共有鍵であり、KeyAは全機器共有の鍵である。

【0009】システム管理者は、システムの運用を開始する時には、ルートの鍵であるKeyAでグループ鍵を暗号化して暗号化鍵情報を生成する。その後何らかの理由で、ある機器をグループからはずす必要が生じた時には、木構造からその機器が保持する鍵を取り除き、分割された複数の小さな木構造のルートの鍵でグループ鍵を暗号化して暗号化鍵情報を生成する。

【0010】例えば、機器1をグループから排除された場合には、グループ鍵は、KeyC、KeyE、k<sub>d2</sub>を用いてそれぞれ暗号化される。ここでの各暗号文を、暗号化鍵情報と呼ぶことにする。グループ鍵を用いて暗号化されたコンテンツとともに、暗号化鍵情報は、コンテンツ供給者から配布される。これを受け取った機器（排除された機器を除く）は、自分が保持する機器鍵に対応した暗号化鍵情報よりグループ鍵を求め、コンテンツを復号する。

【0011】また、非特許文献2は、予め機器が保有している機器鍵の増加を抑えながら、記録媒体に記録され

る鍵情報のサイズを小さくできる木構造パターン分割方式を開示している。

#### 【0012】

【非特許文献2】「デジタルコンテンツ保護用鍵管理方式 “木構造パターン分割方式” (Key management system for digital content protection “Tree pattern division method”)」(中野稔久、大森基司、松崎なつめ、館林誠著) ——SCIS 2002, The 2002 Symposium on Cryptography and Information Security Shirahama, Japan, Jan. 29–Feb. 1, 2002. The Institute of Electronics, Information and Communication Engineers

#### 【0013】

【発明が解決しようとする課題】ところで、現在、運営主体、配信するコンテンツの種類、パッケージメディア、放送、インターネットなどの配信経路や媒体、提供されるサービスなどが異なる様々な複数のコンテンツ配信システムが、それぞれ独自の鍵管理方式を用いて、運営されているという問題がある。

【0014】本発明は、1個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の鍵管理を行うことができるデータ配信システム、鍵管理装置、暗号化装置、利用者機器、これらを実現する方法、コンピュータプログラム及びコンピュータプログラムを記録している記録媒体を提供することを目的とする。

#### 【0015】

【課題を解決するための手段】本発明は、データを暗号化する複数の暗号化装置と、対応する暗号化装置用機器鍵を用いて暗号化データを復号する複数の機器からなるデータ配信システムであって、前記暗号化装置は、データを暗号化して機器に送付すると共に、前記暗号化装置用機器鍵を管理し、さらに公開簿を生成して機器に公開し、前記機器は、前記暗号化装置に対応した、暗号化装置用機器鍵と公開簿を用いて、前記暗号化データを復号することを特徴とする。

【0016】ここで、前記データ配信システムは、前記公開簿が、前記暗号化装置に対応したWebページ、又はパッケージメディアを介して、機器に供給されるように構成してもよい。ここで、前記データ配信システムは、前記公開簿のうち、当該機器に対応したデータだけを切り出して機器に供給する構成してもよい。

【0017】ここで、前記データ配信システムは、さらに、鍵管理機関を備え、前記鍵管理機関は、各暗号化装置に対応した各機器の暗号化装置用機器鍵を生成し、各機器と各暗号化装置に、対応した暗号化装置用機器鍵を供給する構成してもよい。ここで、前記データ配信システムにおける前記鍵管理機関は、各機器の機器鍵を生成して機器に供給し、機器側にて前記機器鍵と暗号化装置に対応した識別情報を一方向性関数に入力し、その出力の暗号化装置用機器鍵を生成する構成して

もよい。

【0018】また、本発明は、データを暗号化して機器に送付する暗号化装置であって、暗号化装置用機器鍵を管理し、さらに公開簿を生成して機器に公開することを特徴とする。ここで、前記暗号化装置は、木構造を構築し、その各ノードに1つ以上のノード鍵を割り当てて、さらに、木構造のリーフに、前記各機器の、暗号化装置用機器鍵を割り当てて、前記暗号化装置用機器鍵とノード鍵を用いて公開簿を生成するように構成してもよい。

【0019】ここで、前記暗号化装置は、前記公開簿に、リーフに割り当てられた暗号化装置用機器鍵のみを用いて、当該リーフからルートに至るノードに対応したノード鍵を順次求めるための情報を載せるように構成してもよい。ここで、前記暗号化装置は、前記公開簿に、あるノードに対応したノード鍵を、そのすべての子ノードに対応したそれぞれのノード鍵で暗号化した暗号文(第1の情報と呼ぶ)を載せるように構成してもよい。

【0020】ここで、前記暗号化装置は、当該ノードの子ノードのうちの1つに対応したノード鍵を予め決められた一方向性関数を用いて変換した結果を、当該ノードに対応したノード鍵とし、公開簿には、これをその他の子ノードに対応したノード鍵で暗号化した暗号文(第2の情報と呼ぶ)を載せるように構成してもよい。ここで、前記暗号化装置は、 $k$ を2以上の整数、 $m$ を0以上の整数とし、各ノード鍵を $(x, y)$ 平面上の点とする場合、共通の親ノードを持つ $k$ 個の全てのノードのノード鍵を結ぶ $(k+m-1)$ 次の曲線を生成し、前記曲線上のノード鍵以外の $(k+m-1)$ 個の点(第3の情報と呼ぶ)を公開簿に載せるように構成してもよい。

【0021】ここで、前記暗号化装置は、前記 $(k+m-1)$ 次の曲線から一方向性関数を用いて予め決められた手法により一意に定まる点を、共通の親ノードに対応したノード鍵とすることを構成してもよい。ここで、前記暗号化装置は、公開鍵暗号の秘密鍵と公開鍵のペアを生成し、秘密鍵を保持して公開鍵を前記公開簿に載せておき、一方、前記木構造のあるノードに対応したノード鍵を、前記公開鍵暗号の秘密鍵で暗号化した結果をその子ノードに対応したノード鍵とすることを構成してもよい。ここで、公開簿に載せる情報を第4の情報と呼ぶ。

【0022】ここで、前記暗号化装置は、秘密の素数 $p$ と $q$ の積 $n$ を計算して、 $p-1$ と $q-1$ の最小公倍数 $L$ を求めて、 $n$ と互いに素となる $L$ 以下の任意の整数 $e$ を求めて、 $L$ を法とする $e$ の逆元 $d$ を求めてこれを秘密鍵とし、前記 $(e, n)$ を公開鍵として公開簿に公開し、さらに、あるノードに対応したノード鍵と、当該ノードからその子ノードに接続する各パスに予め定められている個別のパス番号の排他的論理和を、前記秘密鍵 $d$ を用いて暗号化し、その結果を当該パスに接続する子ノードに対応したノード鍵とすることを構成してもよい。

【0023】ここで、前記暗号化装置は、木構造のリーフ

とそのすぐ上位のノードの間に閲では、前記第1、第2、又は第3の情報を公開簿に載せ、それ以外のノードの間に閲では、前記第4の情報を公開簿に載せるように構成してもよい。また、本発明は、暗号化装置により生成された暗号化データを復号する機器であって、暗号化装置用機器鍵と、前記暗号化装置に対応した公開簿を用いて、前記暗号化データを復号することを特徴とする。

【0024】ここで、前記機器は、個別の機器鍵を保持し、前記機器鍵と前記暗号化装置の識別情報を用いて、対応する暗号化装置用機器鍵を生成するように構成してもよい。ここで、前記機器は、前記暗号化装置が定めた木構造のリーフに割り当てられ、対応した暗号化装置用機器鍵を保持するように構成してもよい。

【0025】ここで、前記機器は、前記暗号化装置に対応した公開簿を用いて、前記木構造における、あるリーフに割り当てられた暗号化装置用機器鍵から、当該のリーフからルートに至るノードに対応したノード鍵を順次求めるように構成してもよい。ここで、前記機器は、前記木構造の、あるノードのノード鍵を用いて、公開簿内の対応する暗号文を復号し、当該ノードの親ノードのノード鍵を求めるように構成してもよい。

【0026】ここで、前記機器は、前記木構造の、あるノードのノード鍵を用いて、公開簿内の対応する暗号文を復号した復号文、又は当該ノードのノード鍵を一方向性関数に入力しその出力値のいずれかを選択して、当該ノードの親ノードのノード鍵として求めるように構成してもよい。ここで、前記機器は、前記木構造の、あるノードのノード鍵と、公開簿内の対応する $(k+m-1)$ 個の点を結ぶ、 $(k+m-1)$ 次の曲線を求め、さらにつこの曲線から一方向性関数を用いて当該ノードの親ノードのノード鍵として求めるように構成してもよい。

【0027】ここで、前記機器は、前記木構造の、あるノードのノード鍵を、公開簿内の対応する公開鍵を用いて復号し、その結果を当該ノードの親ノードのノード鍵とするように構成してもよい。ここで、前記機器は、前記暗号化装置が、秘密の素数 $p$ と $q$ の積 $n$ を計算して、 $p-1$ と $q-1$ の最小公倍数 $L$ を求めて、 $n$ と互いに素となる $L$ 以下の任意の整数 $e$ を求めて、 $L$ を法とする $e$ の逆元 $d$ を求めて秘密鍵とし、前記 $(e, n)$ を公開鍵として公開簿に公開するとき、前記機器は、前記木構造のあるノードのノード鍵を、前記公開鍵 $(e, n)$ を用いて復号し、その結果と、当該ノードの親ノードに接続するパスのパス番号の排他的論理和を求めた結果を、当該ノードの親ノードに対応したノード鍵とするように構成してもよい。

【0028】ここで、前記機器は、前記暗号化装置が、前記第1、第2又は第3の情報を載せた公開簿を用いて、木構造のリーフからそのすぐ上位のノードのノード鍵を求めて、第4の情報を載せた公開簿を用いて、さらに

上位のノードのノード鍵を順次求めるように構成してもよい。

### 【0029】

【発明の実施の形態】1. 暗号化データ配信システム1  
本発明に係る1個の実施の形態としての暗号化データ配信システム1について説明する。

#### 1. 1 暗号化データ配信システム1の構成

暗号化データ配信システム1は、図1に示すように、鍵管理装置100、音楽配信システム管理装置200、音楽コンテンツ配信装置300、公開簿サーバ装置400、DVD供給システム管理装置500、DVD供給装置600、公開簿供給装置700、映画放送システム管理装置800、映画コンテンツ供給装置900、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9、利用者機器1100、図示していない他の複数の利用者機器及び製造装置1200から構成されている。

【0030】鍵管理装置100は、製造装置1200を介して、利用者機器1100に固有の機器鍵kdiを利用者機器1100へ配布する。また、鍵管理装置100は、機器鍵kdiに基づいて生成したシステム用機器鍵Skdi<sup>(1)</sup>、Skdi<sup>(2)</sup>及びSkdi<sup>(3)</sup>をそれぞれ、音楽配信システム管理装置200、DVD供給システム管理装置500及び映画放送システム管理装置800へ配布する。

【0031】音楽配信システム2は、インターネット5を介して音楽のコンテンツを利用者に配信するコンテンツ供給システムであって、音楽配信システム管理装置200、音楽コンテンツ配信装置300、公開簿サーバ装置400、利用者機器1100及び他の利用者機器を含んで構成されている。音楽配信システム管理装置200は、音楽配信システム2において用いられる暗号化のための鍵を管理し、後述する音楽用公開簿を公開簿サーバ装置400を介して、利用者機器1100等に公開する。音楽コンテンツ配信装置300は、音楽配信システム管理装置200により管理されている鍵に基づいて、音楽のコンテンツを暗号化して利用者機器1100等へ送信する。利用者機器1100等は、自分が記憶している機器鍵kdi及び音楽用公開簿に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生する。

【0032】また、DVD供給システム3は、映画などのコンテンツが記録されているDVDを利用者に供給するコンテンツ供給システムであって、DVD供給システム管理装置500、DVD供給装置600、公開簿供給装置700、利用者機器1100及び他の利用者機器を含んで構成されている。DVD供給システム管理装置500は、DVD供給システム3において用いられる暗号化のための鍵を管理し、後述するDVD用公開簿を、公開簿供給装置700を介して、利用者機器1100等に公開する。DVD供給装置600は、DVD供給システ

ム管理装置500により管理されている鍵に基づいて、映画のコンテンツを暗号化してDVDに記録し、暗号化映画コンテンツが記録されたDVDは、利用者に供給される。利用者機器1100等は、自分が記憶している機器鍵kdi及びDVD用公開簿に基づいて、DVDに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生する。

【0033】さらに、映画放送システム4は、映画などのコンテンツを放送波に載せて利用者に供給するコンテンツ供給システムであって、映画放送システム管理装置800、映画コンテンツ供給装置900、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9、利用者機器1100及び他の利用者機器を含んで構成されている。映画放送システム管理装置800は、映画放送システム4において用いられる暗号化のための鍵を管理し、送信装置1000及び放送衛星6を介して、後述する映画用公開簿を放送波により放送することにより、利用者機器1100等に公開する。映画コンテンツ供給装置900は、映画放送システム管理装置800により管理されている鍵に基づいて、映画のコンテンツを暗号化し、送信装置1000及び放送衛星6を介して、暗号化映画コンテンツを放送波により放送することにより、利用者に供給する。利用者機器1100等は、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自分が記憶している機器鍵kdi及び映画用公開簿に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。

#### 【0034】1. 2 鍵管理装置100の構成

鍵管理装置100は、鍵管理機関が有しており、鍵管理機関により管理及び運営がされている。鍵管理機関は、各利用者機器の機器鍵を生成して管理する信頼のおける機関である。鍵管理装置100は、利用者機器1100に固有の機器鍵kdiを生成し、生成した機器鍵kdiを、製造装置1200を介して、利用者機器1100へ配布する。ここで、鍵管理装置100により生成された機器鍵kdiが、可搬型の記録媒体に書き込まれ、鍵管理装置100を有する鍵管理機関は、前記記録媒体を製造装置1200を有する製造業者に手渡す。なお、鍵管理装置100と製造装置1200とは、通信回線により接続されており、鍵管理装置100は、前記通信回線を介して製造装置1200へ、機器鍵kdiを安全な通信プロトコルを用いて、送信するとしてもよい。

【0035】また、鍵管理装置100は、それぞれ、音楽配信システム管理装置200、DVD供給システム管理装置500及び映画放送システム管理装置800と通信回線により接続されている。鍵管理装置100は、機器鍵kdiに基づいて、それぞれ、音楽配信システム管理装置200、DVD供給システム管理装置500及び映画放送システム管理装置800で用いるためのシステム用機器鍵Skdi<sup>(1)</sup>、Skdi<sup>(2)</sup>及びSkdi<sup>(3)</sup>

$s_k d_i^{(3)}$  を生成し、生成したシステム用機器鍵  $S_k d_i^{(1)}$  、  $S_k d_i^{(2)}$  及び  $S_k d_i^{(3)}$  をそれぞれ、前記通信回線を介して、安全な通信プロトコルを用いて、音楽配信システム管理装置 200、DVD供給システム管理装置 500 及び映画放送システム管理装置 800 へ送信する。

【0036】鍵管理装置 100 は、図 2 に示すように、入力部 101、制御部 102、表示部 103、機器鍵生成部 104、システム用機器鍵生成部 105、機器鍵出力部 106、情報記憶部 107 及びシステム用機器鍵送信部 108 から構成されている。鍵管理装置 100 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、通信ユニットなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵管理装置 100 は、その機能を達成する。

【0037】(1) 情報記憶部 107

情報記憶部 107 は、機器鍵管理テーブル 111 及びシステム用機器鍵管理テーブル 121 を有する。

(機器鍵管理テーブル 111) 機器鍵管理テーブル 111 は、図 3 に示すように、機器 ID と機器鍵  $k_d i$  とかなる機器情報を複数個記憶するための領域を備えている。

【0038】機器 ID は、利用者機器を識別するための識別情報であり、具体的には、利用者機器の製造番号である。機器鍵  $k_d i$  は、当該利用者機器に割り当てられる固有の鍵情報である。

(システム用機器鍵管理テーブル 121) システム用機器鍵管理テーブル 121 は、図 4 に示すように、機器 ID とシステム ID とシステム用機器鍵  $S_k d_i^{(1)}$  とかなるシステム情報を複数個記憶するための領域を備えている。

【0039】機器 ID は、上述したように、利用者機器を識別するための識別情報である。システム ID は、音楽配信システム 2、DVD 供給システム 3 及び映画放送システム 4 に代表されるような、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。ここでは、具体的には、音楽配信システム 2、DVD 供給システム 3 及び映画放送システム 4 を識別するシステム ID は、それぞれ、「1」、「2」及び「3」である。

【0040】システム用機器鍵  $S_k d_i^{(1)}$  は、各コンテンツ供給システムにおいて、利用者機器に割り当てられる固有の鍵情報である。 $S_k d_i^{(1)}$  において、サフィックス  $i$  は、当該利用者機器の機器 ID に対応するものであり、サフィックス  $j$  は、当該コンテンツ供給システムのシステム ID に対応するものである。

## (2) 制御部 102

制御部 102 は、機器鍵及びシステム用機器鍵の生成が終了するまで、機器鍵及びシステム用機器鍵の生成の処理を繰り返すように、鍵管理装置 100 の各構成部を制御する。

【0041】また、制御部 102 は、鍵管理機関の運営者から入力部 101 を介して、システム ID 及び機器 ID の入力を受け付ける。制御部 102 は、機器 ID の入力を受け付けると、機器鍵管理テーブル 111 内に、入力を受け付けた前記機器 ID が記憶されているか否かを判断し、前記機器 ID が機器鍵管理テーブル 111 に記憶されていないと判断する場合に、機器 ID を機器鍵生成部 104 へ出力し、機器鍵生成部 104 に対して機器鍵を新たに生成するように指示する。

【0042】一方、制御部 102 は、入力を受け付けた前記機器 ID が機器鍵管理テーブル 111 に記憶されていると判断する場合に、機器鍵管理テーブル 111 から前記機器 ID を含む機器情報を読み出し、読み出した機器情報から機器鍵  $k_d i$  を抽出し、抽出した機器鍵  $k_d i$  をシステム用機器鍵生成部 105 へ出力する。

## (3) 機器鍵生成部 104

機器鍵生成部 104 は、制御部 102 から機器 ID 及び機器鍵を新たに生成する旨の指示を受け取る。

【0043】前記指示を受け取ると、機器鍵生成部 104 は、乱数を生成し、生成した乱数を用いて、新たに機器鍵  $k_d i$  を生成する。次に、機器鍵生成部 104 は、受け取った機器 ID と生成した機器鍵  $k_d i$  とを機器鍵出力部 106 へ出力し、生成した機器鍵  $k_d i$  をシステム用機器鍵生成部 105 へ出力し、受け取った前記機器 ID と生成した機器鍵  $k_d i$  とから構成される機器情報を機器鍵管理テーブル 111 へ書き込む。

【0044】(4) システム用機器鍵生成部 105  
システム用機器鍵生成部 105 は、機器鍵生成部 104 から機器鍵  $k_d i$  を受け取り、制御部 102 からシステム ID を受け取り、受け取った機器鍵  $k_d i$  とシステム ID とを結合して結合情報を得、得られた結合情報に一方向性関数  $h$  を施して、システム用機器鍵  $S_k d_i^{(1)}$  を生成する。

【0045】システム用機器鍵  $S_k d_i^{(1)} = h(k_d i, \text{システム ID})$

ここで、 $h(A, B)$  は、A と B との結合情報に一方向性関数  $h$  を施すことを示す。また、一方向性関数  $h$  の一例は、SHA-1 である。次に、システム用機器鍵生成部 105 は、システム ID 及び生成したシステム用機器鍵  $S_k d_i^{(1)}$  をシステム用機器鍵送信部 108 へ出力する。

【0046】また、システム用機器鍵生成部 105 は、機器 ID、システム ID 及びシステム用機器鍵  $S_k d_i^{(1)}$  を対応付けて構成されるシステム情報をシステム用機器鍵管理テーブル 121 へ書き込む。

## (5) 機器鍵出力部106

機器鍵出力部106は、機器鍵生成部104から機器ID及び機器鍵kdiを受け取り、利用者機器に機器鍵が割り当てられていない場合に、機器ID及び機器鍵kdiを製造装置1200を介して利用者機器へ出力する。

## 【0047】(6) システム用機器鍵送信部108

システム用機器鍵送信部108は、通信回線を介して、音楽配信システム管理装置200、DVD供給システム管理装置500及び映画放送システム管理装置800と接続されている。システム用機器鍵送信部108は、システム用機器鍵生成部105からシステムID及びシステム用機器鍵S<sub>kdi</sub><sup>(1)</sup>を受け取り、制御部102から機器IDを受け取る。次に、システム用機器鍵送信部108は、システムIDにより示されるシステム用管理装置へ、通信回線を介して、機器IDとシステム用機器鍵S<sub>kdi</sub><sup>(1)</sup>を送信する。

## 【0048】(7) 入力部101

入力部101は、鍵管理機関の運営者から、システムID及び機器IDの入力を受け付け、入力を受け付けたシステムID及び機器IDを制御部102へ出力する。

## (8) 表示部103

表示部103は、各種情報を表示する。

## 【0049】1.3 音楽配信システム管理装置200の構成

音楽配信システム管理装置200は、音楽配信システム2において用いられる暗号化のための鍵を管理し、暗号化のためのノード鍵を音楽コンテンツ配信装置300へ出力し、また後述する音楽用公開簿を公開簿サーバ装置400を介して、利用者機器1100等に公開する。

【0050】音楽配信システム管理装置200は、図5に示すように、表示部201、制御部202、入力部203、木構造構築部204、ノード鍵生成部205、公開簿生成部206、送受信部207及び情報記憶部208から構成されている。音楽配信システム管理装置200は、鍵管理装置100と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽配信システム管理装置200は、その機能を達成する。

## 【0051】(1) 情報記憶部208

情報記憶部208は、音楽配信用木構造テーブル211及び音楽用公開簿221を有している。音楽配信用木構造テーブル211は、図6に一例として示す木構造T100に対応しており、木構造T100を表現するためのデータ構造を示している。

【0052】後述するように、木構造構築部204により、木構造T100を表現するためのデータ構造が音楽配信用木構造テーブル211として生成され、情報記憶部208に書き込まれる。

(木構造T100) 木構造T100は、図6に示すように、階層1から階層4までの4階層からなる2分木であ

る。木構造T100は、2分木であるので、木構造T100が有する各ノード（リーフを除く）は、2本のパスを介して下位側の2個のノードにそれぞれ接続されている。階層1にはルートである1個のノードが含まれ、階層2には2個のノードが含まれ、階層3には4個のノードが含まれ、階層4にはリーフである8個のノードが含まれている。なお、木構造において下位側とはリーフ側を示し、上位側とはルート側を示している。

【0053】木構造T100が有する各ノード（リーフを除く）と、下位側のノードとを接続する複数のパスについて、左側のパスから右側のパスへの順に、「1」、「2」、「3」などの番号が割り当てられている。ここで、図6の紙面において、各ノードを中心として当該ノードから左側下方に接続されているパスを左のパスと称し、当該ノードから右側下方に接続されているパスを右のパスと称している。

【0054】各ノードには、ノード番号が付されている。階層1に属するルートであるノードのノード番号は、「1」である。また、階層2を含め、階層2より下位にある階層に属するノードに対しては、左側のノードから右側のノードへの順に、「1」、「2」、「3」などの番号が割り当てられている。ここで、左及び右とは、上述した通りである。例えば、階層2に属する2個のノードのノード番号は、それぞれ「1」と「2」である。また、階層3に属する4個のノードのノード番号は、それぞれ「1」、「2」、「3」及び「4」である。

【0055】また、木構造T100が有する各ノードのうち、最下層に属するノード、即ちリーフには、それぞれ、リーフ番号が割り当てられている。具体的には、図6に示すように、階層4に属する8個のリーフ（ノード番号は、「1」、「2」、「3」、「4」、「5」、「6」、「7」、「8」）には、それぞれ、リーフ番号「000」、「001」、「010」、「011」、「100」、「101」、「110」、「111」が割り当てられている。ここで、リーフ番号は、2進数により表現されている。

【0056】ここで、リーフ番号の定め方について説明する。木構造T100が有する各ノード（リーフを除く）と、下位に接続されるノードとを接続する2本のパスのうち、その一方である左のパスには、「0」の番号を割り当て、他方である右のパスには「1」の番号を割り当てる。これらの番号は、2進数により表現される1ビットの値である。このような規則により、木構造T100が有する全てのパスに、「0」又は「1」の番号を割り当てるすると、ルートからあるリーフへたどる経路に含まれる複数のパスにそれぞれ割り当てられた番号を用いて、ルートから前記リーフへたどる前記経路を一意に識別することができる。このルートから前記リーフへたどる前記経路は、前記リーフに一対一に対応しているので、これらの番号は、前記リーフを識別するとも言える。

【0057】リーフ番号は、ルートから当該リーフへたどる経路に含まれる複数のパスにそれぞれ割り当てられた番号を、この順序で並べることにより、構成される。例えば、リーフ番号「000」は、ルートから左のパスをたどって、階層2のノードに至り、さらに左のパスをたどって、階層3のノードに至り、さらに左のパスをたどって至る階層4のリーフを示している。

【0058】木構造T100が有する各ノードには、ノード鍵が割り当てられる。具体的には、図6に示すように、階層1に属するルートには、ノード鍵「Key A<sup>(1)</sup>」が割り当てられる。また、階層2に属する2個のノード（ノード番号は、「1」及び「2」）には、それぞれ、ノード鍵「Key B<sup>(1)</sup>」及びノード鍵「Key C<sup>(1)</sup>」が割り当てられる。階層3及び階層4に属するノードについても同様である。

【0059】また、木構造T100が有する各リーフには、利用者機器が割り当てられる。具体的には、図6に示すように、各リーフに、利用者機器を識別する機器IDが割り当てられる。

（音楽配信用木構造テーブル211）音楽配信用木構造テーブル211は、図7に示すように、木構造T100に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T100を構成する各ノードにそれぞれ対応している。

【0060】各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リーフについては、階層番号、ノード番号、ノード鍵及び機器IDを含む。階層番号は、当該ノード情報に対応するノードが属する階層を示す番号である。

【0061】ノード番号は、前記階層内において、当該ノード情報に対応するノードを識別するための番号である。ノード鍵は、当該ノード情報に対応するノードに対して割り当てられた鍵である。また、機器IDは、リーフであるノードに対応するノード情報のみに含まれ、リーフ以外のノードに対応するノード情報には含まれない。機器IDは、リーフに割り当てられる利用者機器を識別する識別情報である。

【0062】（音楽用公開簿221）音楽用公開簿221は、図8に示すように、システムID及び所定数個の公開情報を含んで構成されている。各公開情報は、インデックス情報及び暗号化ノード鍵を含む。ここで、前記所定数は、木構造T100に含まれるノード（リーフを除く）の個数の2倍の数であり、木構造T100に含まれる各ノードは、音楽用公開簿221に含まれる2個の公開情報に対応している。

【0063】システムIDは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。インデックス情報は、階層番号及びパス番号を含む。ここで、階層番号は、当該公開情報に対応するノードが属する階層

を示す番号である。また、パス番号は、当該公開情報に応するノードから下位のノードへのパスを示す番号である。木構造T100は、2分木であるので、各ノード（リーフを除く）から下位のノードへのパスは、2本存在する。

【0064】暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、対応するパス番号により示されるパスにより接続される下位ノードに割り当てられたノード鍵を鍵として、暗号化アルゴリズムE1を施して生成されたものである。ここで、暗号化アルゴリズムE1は、一例として、DES(Data Encryption Standard)によるものである。

【0065】また、この明細書において、鍵Aを用いて、平文Bに暗号化アルゴリズムE1を施して得られる暗号文をE1(A, B)と表現する。音楽用公開簿221に含まれる公開情報の一例は、図8に示すように、(3, 1)及びE1(Skd1<sup>(1)</sup>, KeyD<sup>(1)</sup>)を含む。ここで、(3, 1)は、階層番号が3であり、パス番号が1であることを示している。また、E1(Skd1<sup>(1)</sup>, KeyD<sup>(1)</sup>)は、Skd1<sup>(1)</sup>を鍵として用いて、KeyD<sup>(1)</sup>に暗号化アルゴリズムE1を施して得られる暗号文であることを示している。

【0066】(2) 木構造構築部204

木構造構築部204は、音楽配信用木構造テーブル211を生成して情報記憶部208へ書き込む。具体的には、木構造構築部204は、木構造T100に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を音楽配信用木構造テーブル211内に書き込む。なお、この時点では、各ノード情報には、ノード鍵及び機器IDは、含まれていない。

【0067】木構造構築部204は、鍵管理装置100から、制御部202を介して、機器ID及びシステム用機器鍵Skdi<sup>(1)</sup>を受け取り、音楽配信用木構造テーブル211において、受け取ったシステム用機器鍵Skdi<sup>(1)</sup>が1個のリーフに対応するよう、受け取った機器ID及びシステム用機器鍵Skdi<sup>(1)</sup>を音楽配信用木構造テーブル211に書き込む。また、前記リーフを示すリーフ番号を制御部202へ出力する。

【0068】このように、木構造において、システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられる。

(3) 制御部202

制御部202は、機器ID及びシステム用機器鍵Skdi<sup>(1)</sup>の受取りが終了するまで、機器ID及びシステム用機器鍵Skdi<sup>(1)</sup>の受取りと、システム用機器鍵の音楽配信用木構造テーブル211への書き込みと、利用者機器へのリーフ番号の送信とを繰り返すように制御する。

50 【0069】制御部202は、鍵管理装置100から送

受信部207を介して、機器ID及びシステム用機器鍵S<sub>k d i</sub><sup>(1)</sup>を受け取り、受け取った機器ID及びシステム用機器鍵S<sub>k d i</sub><sup>(1)</sup>を木構造構築部204へ出力する。また、制御部202は、木構造構築部204からリーフ番号を受け取り、送受信部207及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID(=1)と受け取ったリーフ番号とを送信する。

【0070】さらに、制御部202は、音楽配信用木構造テーブル211から、所定の基準に基づいて、1個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。なお、ここで選択したノード鍵をデバイス鍵と称することもある。次に、制御部202は、選択したノード鍵を、音楽コンテンツ配信装置300へ送信する。前記デバイス鍵は、利用者機器がコンテンツを復号する際に基づく鍵である。このように、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵が決定される。

#### 【0071】(4) ノード鍵生成部205

制御部202が、機器ID及びシステム用機器鍵S<sub>k d i</sub><sup>(1)</sup>の受取りが終了したと判断する場合に、ノード鍵生成部205は、音楽配信用木構造テーブル211の各ノード(リーフを除く)について、乱数を生成し、生成した乱数を用いてノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、音楽配信用木構造テーブル211へ書き込む。

#### 【0072】(5) 公開簿生成部206

公開簿生成部206は、音楽用公開簿221を生成し、生成した音楽用公開簿221を情報記憶部208に書き込み、生成した音楽用公開簿221を、公開簿サーバ装置400へ送信する。なお、公開簿生成部206による音楽用公開簿221の生成の詳細については、後述する。

#### 【0073】(6) 送受信部207

送受信部207は、通信回線を介して、音楽コンテンツ配信装置300と接続され、また、インターネット5を介して、利用者機器1100と接続されている。送受信部207は、制御部202と音楽コンテンツ配信装置300との間で情報の送受信を行う。また、送受信部207は、制御部202と利用者機器1100との間で情報の送受信を行う。

#### 【0074】(7) 表示部201及び入力部203

表示部201は、制御部202の制御の元に各種の情報を表示する。また、入力部203は、音楽配信システム管理装置200の管理者からの情報の入力を受け付ける。

#### 1.4 公開簿サーバ装置400の構成

公開簿サーバ装置400は、音楽配信システム管理装置

200と通信回線を介して接続されており、通信回線を介して、音楽配信システム管理装置200から音楽用公開簿を受信し、受信した音楽用公開簿を内部に記憶する。また、公開簿サーバ装置400は、インターネット5を介して、利用者機器1100と接続されており、利用者機器1100からの要求に応じて、内部に記憶している音楽用公開簿を、インターネット5を介して、利用者機器1100へ送信する。

【0075】公開簿サーバ装置400は、図9に示すように、情報記憶部401、送受信部402、制御部403、入力部404及び表示部405から構成されている。公開簿サーバ装置400は、鍵管理装置100と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、公開簿サーバ装置400は、その機能を達成する。

【0076】情報記憶部401は、情報を記憶するための領域を備える。送受信部402は、通信回線を介して、音楽配信システム管理装置200と接続されている。また、送受信部402は、インターネット5を介して、利用者機器1100と接続されている。制御部403は、音楽配信システム管理装置200から、通信回線及び送受信部402を介して、音楽用公開簿を受信し、受信した音楽用公開簿を情報記憶部401へ書き込む。

【0077】また、制御部403は、利用者機器1100から、インターネット5を介して、音楽用公開簿の送信要求を受け取る。前記送信要求を受け取ると、制御部403は、情報記憶部401から音楽用公開簿を読み出し、読み出した音楽用公開簿を、インターネット5を介して、利用者機器1100へ送信する。入力部404は、公開簿サーバ装置400の管理者からの入力を受け付ける。

【0078】表示部405は、制御部403の制御により各種の情報を表示する。

#### 1.5 音楽コンテンツ配信装置300の構成

音楽コンテンツ配信装置300は、音楽配信システム管理装置200から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて音楽情報を暗号化し、暗号化グループ鍵及び暗号化音楽情報を、利用者機器1100へ送信する。

【0079】音楽コンテンツ配信装置300は、図10に示すように、情報記憶部301、グループ鍵生成部302、暗号化部303、ノード鍵取得部304、暗号化部305、送受信部306、制御部307、入力部308及び表示部309から構成されている。図10において、各ブロックは、音楽コンテンツ配信装置300の構成要素を示しており、接続線により他のブロックと接続されている。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部305を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部305へ鍵と

しての情報が伝達される経路を示している。暗号化部303を示すブロックについても同様である。また、他の図面についても同様である。

【0080】音楽コンテンツ配信装置300は、鍵管理装置100と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽コンテンツ配信装置300は、その機能を達成する。

#### (1) 情報記憶部301

情報記憶部301は、予め、複数個の音楽情報を記憶している。

#### (2) ノード鍵取得部304

ノード鍵取得部304は、通信回線を介して、音楽配信システム管理装置200に接続されており、音楽配信システム管理装置200から、通信回線を介して、ノード鍵を受信し、受信したノード鍵を、ノード鍵Nkとして暗号化部305へ出力する。

#### (3) グループ鍵生成部302

グループ鍵生成部302は、乱数を生成し、生成した乱数を用いて、グループ鍵Gを生成し、生成したグループ鍵Gを暗号化部305及び暗号化部303へ出力する。

#### (4) 暗号化部305

暗号化部305は、ノード鍵取得部304からノード鍵Nkを受け取り、グループ鍵生成部302からグループ鍵Gを受け取る。

【0081】次に、暗号化部305は、受け取ったノード鍵Nkを用いて、受け取ったグループ鍵Gに暗号化アルゴリズムE3を施して、暗号化グループ鍵E3(Nk, G)を生成する。ここで、暗号化アルゴリズムE3は、一例としてDESによるアルゴリズムである。

【0082】次に、暗号化部305は、生成した暗号化グループ鍵E3(Nk, G)を送受信部306へ出力する。

#### (5) 暗号化部303

暗号化部303は、情報記憶部301から音楽情報をMCを読み出し、また、グループ鍵生成部302からグループ鍵Gを受け取る。

【0083】グループ鍵Gを受け取ると、暗号化部303は、受け取ったグループ鍵Gを鍵として用いて、読み出した音楽情報をMCに暗号化アルゴリズムE2を施して、暗号化音楽情報をE2(G, MC)を生成する。ここで、暗号化アルゴリズムE2は、一例としてDESによるアルゴリズムである。

【0084】次に、暗号化部303は、生成した暗号化音楽情報をE2(G, MC)を送受信部306へ出力する。

#### (6) 送受信部306

送受信部306は、暗号化部305から暗号化グループ鍵E3(Nk, G)を受け取り、暗号化部303から暗号化音楽情報をE2(G, MC)を受け取る。

【0085】次に、送受信部306は、利用者機器1100から受け取った当該利用者の要求に応じて、暗号化グループ鍵E3(Nk, G)と暗号化音楽情報をE2(G, MC)とを、インターネット5を介して、利用者機器1100へ送信する。

(7) 制御部307、入力部308及び表示部309制御部307は、音楽コンテンツ配信装置300の各構成要素を制御する。入力部308は、音楽コンテンツ配信装置300の管理者からの入力を受け付ける。表示部309は、各種の情報を表示する。

#### 【0086】1. 6 DVD供給システム管理装置500の構成

DVD供給システム管理装置500は、DVD供給システム3において用いられる暗号化のための鍵を管理し、後述するDVD用公開簿を、公開簿供給装置700を介して、利用者機器1100等に公開する。DVD供給システム管理装置500は、図11に示すように、表示部501、制御部502、入力部503、木構造構築部504、ノード鍵生成部505、公開簿生成部506、送受信部507及び情報記憶部508から構成されている。

【0087】DVD供給システム管理装置500は、鍵管理装置100と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、DVD供給システム管理装置500は、その機能を達成する。

#### (1) 情報記憶部508

情報記憶部508は、DVD用木構造テーブル511及びDVD用公開簿521を有している。

【0088】DVD用木構造テーブル511は、図13に一例として示す木構造T200に対応しており、木構造T200を表現するためのデータ構造を示している。後述するように、木構造構築部504により、木構造T200を表現するためのデータ構造がDVD用木構造テーブル511として生成され、情報記憶部508に書き込まれる。

【0089】(木構造T200)木構造T200は、図13に示すように、階層1から階層4までの4階層からなる2分木である。木構造T200は、木構造T100と同様の構造を有しているので、詳細の説明は、省略する。

(DVD用木構造テーブル511)DVD用木構造テーブル511は、図12に示すように、木構造T200に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T200を構成する各ノードにそれぞれ対応している。DVD用木構造テーブル511は、音楽配信用木構造テーブル211と同じデータ構造を有している。

【0090】各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リ

ーフについては、階層番号、ノード番号、ノード鍵及び機器IDを含む。なお、階層番号、ノード番号、ノード鍵及び機器IDについては、上述しているので、説明を省略する。

(DVD用公開簿521) DVD用公開簿521は、図14に示すように、システムID及び所定数個の公開情報と構成されている。各公開情報は、インデックス情報及び暗号化ノード鍵を含む。

【0091】ここで、前記所定数は、木構造T200に含まれるノード(リーフを除く)の個数であり、木構造T200に含まれる各ノード(リーフを除く)は、それぞれ、DVD用公開簿521に含まれる公開情報に対応している。システムIDは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

【0092】インデックス情報は、階層番号及びノード番号を含む。ここで、階層番号は、当該公開情報に対応するノードが属する階層を示す番号である。また、ノード番号は、当該公開情報に対応するノードを示す番号である。暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、当該ノードの右下側に接続する下位ノードに割り当てられたノード鍵を鍵として用いて、暗号化アルゴリズムE4を施して生成されたものである。

【0093】ここで、暗号化アルゴリズムE4は、一例として、DESによるものである。DVD用公開簿521に含まれる公開情報の一例は、図14に示すように、(3、1)及びE4(Skd2<sup>(2)</sup>、KeyD<sup>(2)</sup>)である。ここで、(3、1)は、階層番号が3であり、ノード番号が1であることを示している。また、E4(Skd2<sup>(2)</sup>、KeyD<sup>(2)</sup>)は、Skd2<sup>(2)</sup>を鍵として用いて、KeyD<sup>(2)</sup>に暗号化アルゴリズムE4を施して得られる暗号文であることを示している。KeyD<sup>(2)</sup>は、インデックス情報(3、1)で示されるノードに割り当てられるノード鍵であり、Skd2<sup>(2)</sup>は、当該ノードの右下側に接続する下位ノードに割り当てられたノード鍵である。

#### 【0094】(2) 木構造構築部504

木構造構築部504は、木構造構築部204と同様であるので、説明を省略する。

#### (3) 制御部502

制御部502は、制御部202と同様であるので、説明を省略する。

#### 【0095】(4) ノード鍵生成部505

ノード鍵生成部505は、DVD用木構造テーブル511の各ノード(リーフを除く)について、ノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、DVD用木構造テーブル511へ書き込む。なお、ノード鍵生成部505によるノード鍵の生成については、後述する。

#### 【0096】(5) 公開簿生成部506

公開簿生成部506は、DVD用公開簿521を生成し、生成したDVD用公開簿521を情報記憶部508に書き込み、生成したDVD用公開簿521を、公開簿供給装置700へ送信する。なお、公開簿生成部506によるDVD用公開簿521の生成については、後述する。

#### 【0097】(6) 送受信部507

送受信部507は、通信回線を介して、DVD供給装置600と接続され、また、インターネット5を介して、利用者機器1100と接続されている。送受信部507は、制御部502とDVD供給装置600との間で情報の送受信を行う。また、送受信部507は、制御部502と利用者機器1100との間で情報の送受信を行う。

#### 【0098】(7) 表示部501及び入力部503

表示部501は、制御部502の制御の元に各種の情報を表示する。また、入力部503は、DVD供給システム管理装置500の管理者からの情報の入力を受け付ける。

#### 1.7 DVD供給装置600の構成

DVD供給装置600は、DVD供給システム管理装置500から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて映画情報を暗号化し、暗号化グループ鍵及び暗号化映画情報を、DVDに書き込む。暗号化グループ鍵及び暗号化映画情報が書き込まれたDVDは、利用者に供給される。利用者は、前記DVDを利用者機器1100へ装着する。

【0099】DVD供給装置600は、音楽コンテンツ配信装置300と同様の構成を有しているので、ここでは、詳細の説明を省略する。

#### 1.8 公開簿供給装置700の構成

公開簿供給装置700は、通信回線を介して、DVD供給システム管理装置500に接続されている。

【0100】公開簿供給装置700は、DVD供給システム管理装置500から通信回線を介して、DVD用公開簿521を受信し、受信したDVD用公開簿521をDVDに書き込む。DVD用公開簿521が書き込まれたDVDは、利用者に供給される。利用者は、前記DVDを利用者機器1100へ装着する。

#### 1.9 映画放送システム管理装置800の構成

映画放送システム管理装置800は、映画放送システム4において用いられる暗号化のための鍵を管理し、送信装置1000及び放送衛星6を介して、後述する映画用公開簿を放送波により放送することにより、利用者機器1100等に公開する。

【0101】映画放送システム管理装置800は、図15に示すように、表示部801、制御部802、入力部803、木構造構築部804、公開簿生成部806、送受信部807及び情報記憶部808から構成されている。映画放送システム管理装置800は、鍵管理装置1000と同様のコンピュータシステムである。マイクロプロ

ロセッサが、コンピュータプログラムに従って動作することにより、映画放送システム管理装置800は、その機能を達成する。

**【0102】(1) 情報記憶部808**

情報記憶部808は、映画放送用木構造テーブル811及び映画用公開簿821を有しており、また、初期値 $x_0$ 、 $x_{31}$ を予め記憶している。映画放送用木構造テーブル811は、図16に一例として示す木構造T300に対応しており、木構造T300を表現するためのデータ構造を示している。

**【0103】**後述するように、木構造構築部804により、木構造T300を表現するためのデータ構造が映画放送用木構造テーブル811として生成され、情報記憶部808に書き込まれる。

(木構造T300) 木構造T300は、図16に示すように、階層1から階層4までの4階層からなる2分木である。木構造T300は、木構造T100と同様の構造を有しているので、詳細の説明は、省略する。

**【0104】**ここで、木構造T300に関連して複数の公開点が存在する。木構造T300に含まれる2個のノード（同一の階層に属し、同一のノードの下位に接続する）にそれぞれ割り当てられた2個のノード鍵を、2次元空間（ $x-y$ 座標系）上の2点とみなし、2点を通る直線L上の1点が公開点である。公開点の $x$ 座標は、予め定められており、その値は、初期値 $x_0$ に等しい。

**【0105】**このように、公開点は、同一の階層に属するノードに割り当てられた2個のノード鍵に関連して求められる。具体的には、図16に示すように、階層2に、関連して、1個の公開点s7が存在し、階層3に、関連して、2個の公開点s5、s6が存在し、階層4に、関連して、4個の公開点s1～s4が存在する。公開点と階層との関係は、以下において、公開点はある階層に属すると表現することがある。

**【0106】**また、公開点は、インデックス情報（階層番号、公開点のノード番号）により示される。ここで、階層番号は、公開点が属する階層を示し、公開点のノード番号は、同一階層内において、公開点を識別するための識別番号である。

(映画放送用木構造テーブル811) 映画放送用木構造テーブル811は、図17に示すように、木構造T300に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T100を構成する各ノードにそれぞれ対応している。

**【0107】**各ノード情報は、リーフを除くノードについては、階層番号、ノード番号及びノード鍵を含み、リーフについては、階層番号、ノード番号、ノード鍵及び機器IDを含む。階層番号、ノード番号、ノード鍵及び機器IDについては、上述したとおりであり、説明を省略する。

(映画用公開簿821) 映画用公開簿821は、図20

に示すように、システムID、初期値 $x_0$ 及び所定数個の公開情報を含んで構成されている。各公開情報は、インデックス情報及び公開点y座標を含む。

**【0108】**ここで、前記所定数は、木構造T300に関連して存在する公開点の数であり、木構造T300に関連して存在する各公開点は、映画用公開簿821に含まれる各公開情報に対応している。システムIDは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

**【0109】**インデックス情報は、階層番号及び公開点のノード番号を含む。ここで、階層番号は、当該公開情報に対応する公開点が属する階層を示す番号である。また、公開点のノード番号は、各階層内において、公開点を識別する番号である。公開点y座標は、公開点のy座標を示す。

(初期値 $x_0$ ) 初期値 $x_0$ は、各公開点のx座標を示す。

**【0110】(2) 木構造構築部804**

木構造構築部804は、映画放送用木構造テーブル811を生成して情報記憶部808へ書き込む。具体的には、木構造構築部804は、木構造T300に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を映画放送用木構造テーブル811内に書き込む。なお、この時点では、各ノード情報には、ノード鍵及び機器IDは、含まれていない。

**【0111】**木構造構築部804は、鍵管理装置100から、制御部802を介して、機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ を受け取り、映画放送用木構造テーブル811において、受け取ったシステム用機器鍵 $S_{kdi}^{(3)}$ が1個のリーフに対応するように、受け取った機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ を映画放送用木構造テーブル811に書き込む。また、前記リーフを示すリーフ番号を制御部802へ出力する。

**【0112】(3) 制御部802**

制御部802は、機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ の受取りが終了するまで、機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ の受取りと、システム用機器鍵の映画放送用木構造テーブル811への書き込みと、利用者機器へのリーフ番号の送信を繰り返す。

**【0113】**制御部802は、鍵管理装置100から送受信部807を介して、機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ を受け取り、受け取った機器ID及びシステム用機器鍵 $S_{kdi}^{(3)}$ を木構造構築部804へ出力する。また、制御部802は、木構造構築部804からリーフ番号を受け取り、送受信部807及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID(=3)と受け取ったリーフ番号とを送信する。

【0114】さらに、制御部802は、映画放送用木構造テーブル811から、所定の基準に基づいて、1個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。次に、制御部802は、選択したノード鍵を、映画コンテンツ供給装置900へ送信する。

【0115】(4) 公開簿生成部806

公開簿生成部806は、映画用公開簿821を生成し、生成した映画用公開簿821を情報記憶部808に書き込み、生成した映画用公開簿821を、送信装置1000へ送信する。また、公開簿生成部806は、木構造T300に含まれる各ノード(リーフを除く)について、ノード鍵を生成し、ノードに割り当てる。

【0116】以下に、公開簿生成部806による映画用公開簿821の生成、ノード鍵の生成及びノードへの割り当てについて、説明する。公開簿生成部806は、システムID(ここでは、「3」)を映画用公開簿821へ書き込む。また、情報記憶部808から初期値 $x_0$ を読み出し、読み出した初期値 $x_0$ を映画用公開簿821へ書き込む。

【0117】次に、公開簿生成部806は、木構造T300の、階層3から階層1まで順に、また、各階層内の各ノードについて順に、以下に示す処理・～・を繰り返す。

- ・公開簿生成部806は、当該ノードの下位に接続する2個の下位ノードに、それぞれ対応する2個のノード情報を映画放送用木構造テーブル811から読み出す。

【0118】ここで、一例として、当該ノードは、インデックス情報(3、1)により示されるノードT301であるとする。木構造T300の一部分であって、T301を含むものを図19に示す。公開簿生成部806は、ノードT301の下位に接続する2個の下位ノードT302、T303に、それぞれ対応する2個のノード情報812、813を映画放送用木構造テーブル811から読み出す。

【0119】・公開簿生成部806は、読み出した2個のノード情報からそれぞれ2個のノード鍵Nk1、Nk2を抽出する

ここで、一例として、公開簿生成部806は、読み出した2個のノード情報812、813から、ノード鍵Skd1<sup>(3)</sup>、Skd2<sup>(3)</sup>を抽出する。

- ・公開簿生成部806は、当該2個のノード鍵Nk1、Nk2をそれぞれ2個の点とみなし、2個の点を通る直線Lを求める。具体的には、ノード鍵Nk1が32ビットで表現される場合に、Nk1の上位16ビットをx座標とし、Nk1の下位16ビットをy座標とし、これら(x座標、y座標)により2次元空間(x-y座標系)上の点を表現する。ノード鍵Nk2についても同様である。

【0120】ここで、一例として、公開簿生成部806は、ノード鍵Skd1<sup>(3)</sup>、Skd2<sup>(3)</sup>による2個の点を通る直線Lを求める。図18に、x-y座標系上のノード鍵Skd1<sup>(3)</sup>、Skd2<sup>(3)</sup>による2個の点を示し、また、直線Lを示している。

- ・公開簿生成部806は、直線L上の点( $x_0$ 、 $s_{(y)}$ )を求める。

【0121】ここで、一例として、公開簿生成部806は、直線L上の点 $s_1$ ( $x_0$ 、 $s_{(y)}$ )を求める。図18に示すように、点 $s_1$ は、ノード鍵Skd1<sup>(3)</sup>、Skd2<sup>(3)</sup>による2個の点を通る直線Lの上に存在している。

- ・公開簿生成部806は、公開点y座標 $s_{(y)}$ を、インデックス情報(階層番号、公開点のノード番号)とともに、映画用公開簿821へ書き込む。

【0122】ここで、一例として、公開簿生成部806は、インデックス情報(4、1)と公開点y座標 $s_1$ <sub>(y)</sub>とを映画用公開簿821へ書き込む。

- ・公開簿生成部806は、直線Lのy切片YIを求める。図18に示すように、直線Lとy軸との交点のy座標は、YIである。

- ・公開簿生成部806は、一方向性関数gを用いて、g(YI)を算出する。

【0123】・公開簿生成部806は、g(YI)をx座標とする直線L上の点のy座標YGを求める。

- ・公開簿生成部806は、求めた点(g(YI)、YG)をノード鍵とし、ノード鍵を当該ノードに対応付けて映画放送用木構造テーブル811へ書き込む。ここで、一例として、KeyD<sup>(3)</sup>=(g(YI)、YG)である。

【0124】以上に説明した処理・～・を繰り返すことにより、図17に一例として示す映画放送用木構造テーブル811のノード(リーフを除く)に対して、ノード鍵が生成されて割り当てられ、また、図20に一例として示す映画用公開簿821が生成される。

(5) 送受信部807

送受信部807は、通信回線を介して、映画コンテンツ供給装置900と接続され、また、通信回線を介して、送信装置1000と接続されている。

【0125】送受信部807は、制御部802と映画コンテンツ供給装置900との間で情報の送受信を行う。また、送受信部807は、制御部202から出力される情報を、送信装置1000、送信用アンテナ10、放送衛星6及び受信用アンテナ9を介して、利用者機器1100へ送信する。

(6) 表示部801及び入力部803

表示部801は、制御部802の制御の元に各種の情報を表示する。また、入力部803は、映画放送システム管理装置800の管理者からの情報の入力を受け付けける。

【0126】1. 10 映画コンテンツ供給装置900 映画コンテンツ供給装置900は、映画放送システム管理装置800から受け取ったノード鍵を用いてグループ鍵を暗号化し、グループ鍵を用いて映画情報を暗号化し、暗号化グループ鍵及び暗号化映画情報を、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9を介して、利用者機器1100へ送信する。

【0127】映画コンテンツ供給装置900は、音楽コンテンツ配信装置300と同様の構成を有しているので、ここでは、詳細の説明を省略する。

1. 11 送信装置1000、放送衛星6  
送信装置1000は、それぞれ、映画放送システム管理装置800及び映画コンテンツ供給装置900と通信回線を介して接続されており、映画放送システム管理装置800及び映画コンテンツ供給装置900からそれぞれ情報を受け取り、受け取った情報を、送信用アンテナ10により電波として放送衛星6へ送信する。

【0128】1. 12 利用者機器1100

利用者機器1100は、自身が記憶している機器鍵kdi及び音楽用公開簿に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生し、自身が記憶している機器鍵kdi及びDVD用公開簿に基づいて、DVDに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生し、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自身が記憶している機器鍵kdi及び映画用公開簿に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。

【0129】利用者機器1100は、図21に示すように、情報記憶部1101、機器鍵記憶部1102、ノード鍵特定部1103、復号部1104、制御部1105、入力部1106、表示部1107、情報抽出部1108、復号部1109、送受信部1110、DVD接続部1111、チューナ部1112及び再生部1113から構成されている。

【0130】利用者機器1100には、受信用アンテナ9、モニタ1115及びスピーカ1116が接続されている。また、利用者機器1100は、インターネット5に接続されている。なお、他の利用者機器については、利用者機器1100と同様の構成を有しているので、説明を省略する。

【0131】(1) 機器鍵記憶部1102

機器鍵記憶部1102は、機器鍵kdi及び機器IDを記憶するための領域を備えている。機器鍵kdi及び機器IDについては、上述した通りであるので、説明を省略する。

【0132】(2) 情報記憶部1101、情報記憶部1101は、システムIDテーブル1151を有し、音楽用公開簿1161、DVD用公開簿1162、映画用公開簿1163、暗号化グループ鍵及び暗号化コンテンツ

を記憶するための領域を備えている。音楽用公開簿、DVD用公開簿、映画用公開簿、暗号化グループ鍵及び暗号化コンテンツについては、上述した通りであるので、説明を省略する。

【0133】システムIDテーブル1151は、システム名、システムID及びリーフ番号からなる組を複数個記憶するための領域を備えている。システム名は、音楽配信システム2、DVD供給システム3及び映画放送システム4などのコンテンツ供給システムを特定するための名称である。システムIDは、上述したように、コンテンツ供給システムをシステムするために識別子である。

【0134】リーフ番号は、対応するコンテンツ供給システムにおいて、利用者機器1100が割り当てられているリーフを示す番号である。

(3) 送受信部1110、DVD接続部1111、チューナ部1112

送受信部1110は、インターネット5と接続されており、外部の装置から情報を受信し、受け取った情報を情報抽出部1108へ出力する。

【0135】DVD接続部1111は、利用者機器1100に装着されたDVDから情報を読み出し、読み出した情報を情報抽出部1108へ出力する。チューナ部1112は、受信用アンテナ9に接続されており、放送波を選択的に受信し、受信した放送波を情報として情報抽出部1108へ出力する。

(4) 入力部1106、入力部1106は、利用者から情報の入力を受け付け、受け付けた情報を制御部1105へ出力する。

【0136】(5) 制御部1105、制御部1105は、利用者から入力部1106を介して、利用するシステム名の入力を受け付ける。前記入力を受け付けると、制御部1105は、情報記憶部1101が有するシステムIDテーブル1151から、入力を受け付けたシステム名に対応するシステムIDを取得する。

【0137】次に、制御部1105は、取得したシステムIDが「1」、「2」又は「3」のいずれであるかを判断する。制御部1105は、システムIDが「1」であると判断する場合に、ノード鍵特定部1103に対して、ノード鍵の特定(1)の処理を行うように制御し、システムIDが「2」であると判断する場合に、ノード鍵の特定(2)の処理を行うように制御し、システムIDが「3」であると判断する場合に、ノード鍵特定部1103に対して、ノード鍵の特定(3)の処理を行うように制御する。

【0138】制御部1105は、コンテンツの取得、復号、再生処理が終了したか否かを判断し、終了していないと判断する場合に、コンテンツの取得、復号、再生処理を繰り返すように、各構成要素を制御する。終了したと判断する場合に、制御部1105は、利用者機器11

00によるコンテンツの取得、復号、再生を終了する。

【0139】(6) 情報抽出部1108

(システムID及びリーフ番号の取得)情報抽出部1108は、音楽配信システム管理装置200から、インターネット5及び送受信部1110を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「音楽配信システム」と対応付けて、システムIDテーブル1151へ書き込む。

【0140】また、情報抽出部1108は、DVD供給システム管理装置500から、インターネット5及び送受信部1110を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「DVD供給システム」と対応付けて、システムIDテーブル1151へ書き込む。また、情報抽出部1108は、映画放送システム管理装置800から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「映画放送システム」と対応付けて、システムIDテーブル1151へ書き込む。

【0141】(公開簿の取得)情報抽出部1108は、公開簿サーバ装置400から、インターネット5及び送受信部1110を介して、音楽用公開簿を受信し、受信した音楽用公開簿を、音楽用公開簿1161として情報記憶部1101へ書き込む。また、利用者によりDVD用公開簿が記録されているDVDが利用者機器1100に装着されると、情報抽出部1108は、装着されたDVDから、DVD接続部1111を介して、DVD用公開簿を読み出し、読み出したDVD用公開簿を、DVD用公開簿1162として情報記憶部1101へ書き込む。

【0142】また、情報抽出部1108は、映画放送システム管理装置800から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、映画用公開簿を受信し、受信した映画用公開簿を、映画用公開簿1163として情報記憶部1101へ書き込む。

(暗号化グループ鍵及び暗号化コンテンツの取得)情報抽出部1108は、音楽コンテンツ配信装置300から、インターネット5及び送受信部1110を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む。

【0143】また、利用者により暗号化グループ鍵及び暗号化コンテンツが記録されているDVDが利用者機器1100に装着されると、情報抽出部1108は、装着されたDVDから、DVD接続部1111を介して、暗号化グループ鍵及び暗号化コンテンツを読み出し、読み出した暗号化グループ鍵及び暗号化コンテンツを、暗号

化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む。

【0144】また、情報抽出部1108は、映画コンテンツ供給装置900から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む。

【0145】(7)復号部1104、ノード鍵特定部1103によるノード鍵の特定が終了すると、復号部1104は、情報記憶部1101から暗号化グループ鍵を読み出し、特定されたノード鍵を鍵として用いて、読み出した暗号化グループ鍵に復号アルゴリズムD3を施して、グループ鍵=D3(ノード鍵、暗号化グループ鍵)を生成する。

【0146】ここで、復号アルゴリズムD3は、暗号化アルゴリズムE3に対応するものであって、暗号化アルゴリズムE3により生成された暗号文を復号する。

(8)復号部1109

復号部1109は、暗号化コンテンツを情報記憶部1101から読み出し、生成されたグループ鍵を鍵として用いて、読み出した暗号化コンテンツに復号アルゴリズムD2を施して、コンテンツ=D2(グループ鍵、暗号化コンテンツ)を生成する。

【0147】ここで、復号アルゴリズムD2は、暗号化アルゴリズムE2に対応するものであって、暗号化アルゴリズムE2により生成された暗号文を復号する。

(9)再生部1113

再生部1113は、モニタ1115及びスピーカ1116に接続されている。再生部1113は、生成されたコンテンツを再生し、モニタ1115及びスピーカ1116に出力する。

(10)表示部1107

表示部1107は、制御部1105の制御により、情報を表示する。

(11)ノード鍵特定部1103

ノード鍵特定部1103は、制御部1105の制御により、次に示すノード鍵の特定(1)の処理、ノード鍵の特定(2)の処理及びノード鍵の特定(3)の処理のうちの何れかを実行する。

【0149】(a)ノード鍵の特定(1)の処理

ノード鍵特定部1103は、情報記憶部1101が有するシステムIDテーブル1151から、システムIDに対応するリーフ番号を読み出し、機器鍵記憶部1102から、機器鍵kdiを読み出す。また、ノード鍵特定部1103は、システムIDに対応する公開簿を特定する。公開簿に含まれているシステムIDと制御部1105により取得したシステムIDとが一致するか否かによ

り、公開簿を特定する。ここでは、システムIDは、「1」であるので、音楽用公開簿1161が特定される。

【0150】次に、ノード鍵特定部1103は、システム用機器鍵 $S_{kdi}^{(1)} = h(kdi, \text{システムID})$ を生成する。ここで、 $h$ は、一方向性関数である。次に、リーフ番号に、「1」を加算して、階層3のパス番号を求める。例えば、リーフ番号が「000」である場合には、「000」に「1」加算すると「001」が得られる。この値は、リーフ番号「000」が示すリーフが接続されるパスの番号と一致する。次に、ノード鍵特定部1103は、インデックス情報=(3、パス番号)を設定し、音楽用公開簿1161から設定したインデックス情報に対応する暗号化ノード鍵を読み出す。次に、システム用機器鍵 $S_{kdi}^{(1)}$ を鍵として用いて、読み出した暗号化ノード鍵を復号する。

#### 【0151】

$$R_3 = D1(S_{kdi}^{(1)}, \text{暗号化ノード鍵})$$

こうして、利用者機器1100に割り当てられたリーフ番号が示すリーフの上側に接続するノードに割り当てられたノード鍵が求められる。以降同様にして、ノード鍵特定部1103は、さらに上位に接続するノードに割り当てられたノード鍵を求める。

【0152】このようにして、ノード鍵特定部1103は、リーフ番号が示すリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求めることができる。次に、ノード鍵特定部1103は、このようにして、求めた複数のノード鍵のうちから1個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

#### 【0153】(b) ノード鍵の特定(2)の処理

ノード鍵特定部1103は、情報記憶部1101が有するシステムIDテーブル1151から、システムIDに対応するリーフ番号を読み出し、機器鍵記憶部1102から、機器鍵 $kdi$ を読み出す。また、ノード鍵特定部1103は、上記と同様にして、システムIDに対応する公開簿を特定する。ここでは、システムIDは、「2」であるので、DVD用公開簿1162が特定される。

【0154】次に、ノード鍵特定部1103は、上記と同様にして、システム用機器鍵 $S_{kdi}^{(2)} = h(kdi, \text{システムID})$ を生成する。次に、ノード鍵特定部1103は、木構造T200の階層4から階層3へ、左パスをたどるか、右パスをたどるかをリーフ番号の最下位ビットの値により、決定する。最下位ビットの値が「0」であるなら、左パスをたどり、最下位ビットの値が「1」であるなら、右パスをたどる。

【0155】また、木構造T200の階層3から階層2へ、左パスをたどるか、右パスをたどるかを決定する場合には、リーフ番号の第2ビットの値により、決定す

る。第2ビットの値が「0」であるなら、左パスをたどり、第2ビットの値が「1」であるなら、右パスをたどる。さらに、木構造T200の階層2から階層1へ、左パスをたどるか、右パスをたどるかを決定する場合には、リーフ番号の最上位ビットの値により、決定する。最上位ビットの値が「0」であるなら、左パスをたどり、最上位ビットの値が「1」であるなら、右パスをたどる。

【0156】このように、リーフ番号の各ビットにより、左パスをたどるか、右パスをたどるかが決定できるのは、リーフ番号の各ビットが元々、左パスか又は右パスにより定められているからである。左パスをたどると決定する場合に、ノード鍵特定部1103は、ノード鍵 $R_3 = g(S_{kdi}^{(2)})$ を求める。

【0157】右パスをたどると決定する場合に、ノード鍵特定部1103は、リーフ番号から階層3のノード番号を求め、インデックス情報=(3、ノード番号)を設定し、DVD用公開簿1162から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し、読み出した暗号化ノード鍵を、 $S_{kdi}^{(2)}$ を鍵として用いて、復号する。こうしてノード鍵 $R_3 = D4(S_{kdi}^{(2)}, \text{暗号化ノード鍵})$ が得られる。

【0158】ノード鍵特定部1103は、上に示した手順を、下位の階層から上位の階層へ向かって繰り返すことにより、リーフ番号により示されるリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求める。次に、ノード鍵特定部1103は、このようにして、求めた複数のノード鍵のうちから1個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

#### 【0159】(c) ノード鍵の特定(3)の処理

ノード鍵特定部1103は、情報記憶部1101が有するシステムIDテーブル1151から、システムIDに対応するリーフ番号を読み出し、機器鍵記憶部1102から、機器鍵 $kdi$ を読み出し、システムIDに対応する公開簿を特定する。ここでは、システムIDは、「3」であるので、映画用公開簿1163が特定される。

【0160】次に、ノード鍵特定部1103は、システム用機器鍵 $S_{kdi}^{(3)} = h(kdi, \text{システムID})$ を生成する。また、映画用公開簿1163から初期値 $x_0$ を読み出す。次に、ノード鍵特定部1103は、リーフ番号から階層4の公開点のノード番号を求める、インデックス情報=(4、公開点のノード番号)を設定し、設定したインデックス情報に対応する公開点 $y$ 座標 $y_4$ を映画用公開簿1163から読み出す。次に、機器鍵 $kdi$ と公開点 $(x_0, y_4)$ を通る直線 $L_4$ を求める、直線 $L_4$ の $y$ 切片 $YI_4$ を求める、 $g(YI_4)$ を求める。次に、 $g(YI_4)$ を $x$ 座標とする直線 $L_4$ 上の点の $y$ 座標 $YG_4$ を求める、 $R_3 = (g(YI_4), YG_4)$ とす

る。このようにしてノード鍵  $R_3$  が得られる。

【0161】ノード鍵特定部1103は、同様の手順を繰り返すことにより、リーフ番号により示されるリーフからルートへの経路上の各ノードに割り当てられたノード鍵を求める。次に、ノード鍵特定部1103は、このようにして、求めた複数のノード鍵のうちから1個のノード鍵を決定する。ここでは、最上位のノード、つまり、ルートに割り当てられたノード鍵を採用することとする。

#### 【0162】1. 1.3 鍵管理装置100の動作

鍵管理装置100の動作について、図22に示すフローチャートを用いて説明する。制御部102は、鍵管理業者から入力部101を介して、システムIDの入力を受け付け（ステップS101）、入力部101を介して、機器IDの入力を受け付ける（ステップS102）。

【0163】次に、制御部102は、機器鍵管理テーブル111内に、入力を受け付けた前記機器IDが記憶されているか否かを判断し、前記機器IDが機器鍵管理テーブル111に記憶されていないと判断する場合に（ステップS103）、制御部102は、機器IDを機器鍵生成部104へ出力し、機器鍵生成部104に対して機器鍵を新たに生成するように指示し、機器鍵生成部104は、新たに機器鍵  $k_{d,i}$  を生成し、機器IDと生成した機器鍵  $k_{d,i}$  を機器鍵出力部106へ出力し、生成した機器鍵  $k_{d,i}$  をシステム用機器鍵生成部105へ出力し、入力を受け付けた前記機器IDと生成した機器鍵  $k_{d,i}$  とから構成される機器情報を機器鍵管理テーブル111へ書き込む（ステップS105）。

【0164】制御部102は、入力を受け付けた前記機器IDが機器鍵管理テーブル111に記憶されていると判断する場合に（ステップS103）、機器鍵管理テーブル111から前記機器IDを含む機器情報を読み出し、読み出した機器情報を機器鍵  $k_{d,i}$  を読み出し、読み出した機器鍵  $k_{d,i}$  をシステム用機器鍵生成部105へ出力する（ステップS104）。

【0165】システム用機器鍵生成部105は、機器鍵生成部104から機器鍵  $k_{d,i}$  を受け取り、制御部102からシステムIDを受け取り、受け取った機器鍵  $k_{d,i}$  とシステムIDとに一方向性関数  $h$  を施して、システム用機器鍵  $S_{k,d,i}^{(0)} = h(k_{d,i}, \text{システムID})$  を生成し、生成したシステム用機器鍵  $S_{k,d,i}^{(0)}$  とシステムIDとをシステム用機器鍵送信部108へ出力する（ステップS106）。

【0166】次に、システム用機器鍵生成部105は、機器ID、システムID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  を対応付けて構成されるシステム情報をシステム用機器鍵管理テーブル121へ書き込む（ステップS107）。次に、機器鍵出力部106は、利用者機器に機器鍵が割り当てられていない場合に、機器IDと機器鍵  $k_{d,i}$  を製造装置1200を介して利用者機器へ出力す

る（ステップS108）。

【0167】次に、システム用機器鍵送信部108は、システムIDにより示されるシステム用管理装置へ、機器IDとシステム用機器鍵  $S_{k,d,i}^{(0)}$  を送信する（ステップS109）。次に、機器鍵及びシステム用機器鍵の生成が終了しているならば（ステップS110）、鍵管理装置100は、処理を終了し、終了していないならば（ステップS110）、ステップS101へ戻って処理を繰り返す。

#### 【0168】1. 1.4 音楽配信システム管理装置200の動作

（1）音楽配信システム管理装置200の全体の動作  
音楽配信システム管理装置200の動作について、図23に示すフローチャートを用いて説明する。木構造構築部204は、音楽配信用木構造テーブル211を生成して情報記憶部208へ書き込む（ステップS121）。

【0169】次に、制御部202は、鍵管理装置100から送受信部207を介して、機器ID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  を受け取り、受け取った機器ID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  を木構造構築部204へ出力する（ステップS122）。次に、木構造構築部204は、音楽配信用木構造テーブル211において、受け取ったシステム用機器鍵  $S_{k,d,i}^{(0)}$  が1個のリーフに対応するように、機器ID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  を音楽配信用木構造テーブル211に書き込む（ステップS123）。次に、制御部202は、送受信部207及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID

（=1）とリーフ番号とを送信する（ステップS124）。

【0170】次に、制御部202は、機器ID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップS125）、ステップS122へ戻って処理を繰り返す。制御部202が、機器ID及びシステム用機器鍵  $S_{k,d,i}^{(0)}$  の受取りが終了したと判断する場合には（ステップS125）、さらに、ノード鍵生成部205は、音楽配信用木構造テーブル211の各ノード（リーフを除く）について、ノード鍵を生成し、生成したノード鍵を各ノードに対応付けて、音楽配信用木構造テーブル211へ書き込む（ステップS126）。

【0171】次に、公開簿生成部206は、音楽用公開簿221を生成し、生成した音楽用公開簿221を情報記憶部208に書き込み（ステップS127）、生成した音楽用公開簿221を、公開簿サーバ装置400へ送信し（ステップS128）、制御部202は、音楽配信用木構造テーブル211から、1個のノード鍵を選択し（ステップS129）、選択したノード鍵を、音楽コンテンツ配信装置300へ送信する（ステップS130）。

## 【0172】(2) 音楽用公開簿の生成の動作

次に、公開簿生成部206による音楽用公開簿の生成の動作について、図24～図25に示すフローチャートを用いて説明する。なお、ここで説明する音楽用公開簿の生成の動作は、図23に示すフローチャートにおけるステップS127の詳細である。

【0173】公開簿生成部206は、システムID（ここでは、「1」）を音楽用公開簿221へ書き込む（ステップS141）。次に、ステップS142からステップS152において、階層3から階層1まで（階層の番号m=3、2、1）、順に、以下に示すステップS143～ステップS151を繰り返す。次に、公開簿生成部206は、ステップS143からステップS151において、階層番号mにより示される階層内の各ノードについて、順に、以下に示すステップS144～ステップS150を繰り返す。

【0174】公開簿生成部206は、当該ノードに対応するノード情報を音楽配信用木構造テーブル211から読み出し（ステップS144）、読み出したノード情報からノード鍵Mkを抽出する（ステップS145）。次に、公開簿生成部206は、当該ノードの直下に接続されている2個の下位ノードにそれぞれ対応する2個のノード情報を、音楽配信用木構造テーブル211から読み出し（ステップS146）、次に、読み出した2個のノード情報のそれからノード鍵k1、k2を抽出する（ステップS147）。さらに、公開簿生成部206は、抽出したノード鍵k1、k2をそれぞれ鍵として用いて、ノード鍵Mkに暗号化アルゴリズムE1を施して、暗号化ノード鍵E1（k1、Mk）、E1（k2、Mk）を生成し（ステップS148）、当該ノードから左下側への経路に対応するインデックス情報（階層番号、パス番号）と暗号化ノード鍵E1（k1、Mk）とを、公開情報として、音楽用公開簿221へ書き込み（ステップS149）、当該ノードから右下側への経路に対応するインデックス情報（階層番号、パス番号）と暗号化ノード鍵E1（k2、Mk）とを、公開情報として、音楽用公開簿221へ書き込む（ステップS150）。

## 【0175】1.15 音楽コンテンツ配信装置300の動作

音楽コンテンツ配信装置300の動作について、図26に示すフローチャートを用いて説明する。ノード鍵取得部304は、音楽配信システム管理装置200から、通信回線を介して、ノード鍵Nkを受信し、受信したノード鍵Nkを暗号化部305へ出力する（ステップS171）。次に、グループ鍵生成部302は、乱数を生成し、生成した乱数を用いて、グループ鍵Gを生成し、生成したグループ鍵Gを暗号化部305及び暗号化部303へ出力する（ステップS172）。次に、暗号化部305は、受け取ったノード鍵Nkを用いて、受け取った

グループ鍵Gに暗号化アルゴリズムE3を施して、暗号化グループ鍵E3（Nk、G）を生成し、生成した暗号化グループ鍵E3（Nk、G）を送受信部306へ出力する（ステップS173）。

【0176】次に、暗号化部303は、情報記憶部301から音楽情報MCを読み出し（ステップS174）、グループ鍵生成部302からグループ鍵Gを受け取り、受け取ったグループ鍵Gを鍵として用いて、読み出した音楽情報MCに暗号化アルゴリズムE2を施して、暗号化音楽情報E2（G、MC）を生成し、生成した暗号化音楽情報E2（G、MC）を送受信部306へ出力する（ステップS175）。

【0177】次に、送受信部306は、暗号化グループ鍵E3（Nk、G）と暗号化音楽情報E2（G、MC）を受け取り、利用者の要求に応じて、受け取った暗号化グループ鍵E3（Nk、G）と暗号化音楽情報E2（G、MC）とを、インターネット5を介して、利用者機器1100へ送信する（ステップS176）。

1.16 DVD供給システム管理装置500の動作  
20 (1) DVD供給システム管理装置500の全体の動作  
DVD供給システム管理装置500の全体の動作について、図27に示すフローチャートを用いて説明する。

【0178】木構造構築部504は、DVD用木構造テーブル511を生成して情報記憶部508へ書き込む（ステップS191）。次に、制御部502は、鍵管理装置100から送受信部507を介して、機器ID及びシステム用機器鍵Skdi<sup>(2)</sup>を受け取り、受け取った機器ID及びシステム用機器鍵Skdi<sup>(2)</sup>を木構造構築部504へ出力する（ステップS192）。次に、木構造構築部504は、DVD用木構造テーブル511において、受け取ったシステム用機器鍵Skdi<sup>(2)</sup>が1個のリーフに対応するように、機器ID及びシステム用機器鍵Skdi<sup>(2)</sup>をDVD用木構造テーブル511に書き込む（ステップS193）。次に、制御部502は、送受信部507及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID（=2）とリーフ番号とを送信する（ステップS194）。

【0179】次に、制御部502は、機器ID及びシステム用機器鍵Skdi<sup>(2)</sup>の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップS195）、ステップS192へ戻って処理を繰り返す。制御部502が、機器ID及びシステム用機器鍵Skdi<sup>(2)</sup>の受取りが終了したと判断する場合には（ステップS195）、さらに、ノード鍵生成部505は、ノード鍵を生成する（ステップS196）。

【0180】次に、公開簿生成部506は、DVD用公開簿521を生成し、生成したDVD用公開簿521を情報記憶部508に書き込み（ステップS197）、生成したDVD用公開簿521を、公開簿供給装置700

へ送信し（ステップS198）、制御部502は、DVD用木構造テーブル511から、1個のノード鍵を選択し（ステップS199）、選択したノード鍵を、DVD供給装置600へ送信する（ステップS200）。

【0181】(2)ノード鍵の生成の動作

次に、ノード鍵生成部505によるノード鍵の生成の動作について、図28に示すフローチャートを用いて説明する。なお、ここで説明するノード鍵の生成の動作は、図27に示すフローチャートにおけるステップS196の詳細である。ノード鍵生成部505は、ステップS211からステップS218において、階層3から階層1まで（階層の番号m=3, 2, 1）、順に、以下に示すステップS212～ステップS217を繰り返す。

【0182】次に、ノード鍵生成部505は、ステップS212からステップS217において、階層番号mにより示される階層内の各ノードについて順に、以下に示すステップS213～ステップS216を繰り返す。ノード鍵生成部505は、当該ノードの下位に接続する2個の下位ノードのうち、左側に接続する下位ノードのノード情報をDVD用木構造テーブル511から読み出す（ステップS213）。

【0183】次に、ノード鍵生成部505は、読み出したノード情報をノード鍵を、ノード鍵N<sub>k</sub>として抽出し（ステップS214）、次に、抽出したノード鍵N<sub>k</sub>に一方向性関数gを施して、新たなノード鍵N<sub>ew=g</sub>（ノード鍵N<sub>k</sub>）を生成し（ステップS215）、新たに生成したノード鍵N<sub>ew</sub>を、当該下位ノードに対応けて、DVD用木構造テーブル511へ書き込む（ステップS216）。

【0184】(3)DVD用公開簿の生成の動作

次に、公開簿生成部506によるDVD用公開簿の生成の動作について、図29～図30に示すフローチャートを用いて説明する。なお、ここで説明するDVD用公開簿の生成の動作は、図27に示すフローチャートにおけるステップS197の詳細である。

【0185】公開簿生成部506は、システムID（ここでは、「2」）をDVD用公開簿521へ書き込む（ステップS231）。次に、ステップS232からステップS241において、階層3から階層1まで（階層の番号m=3, 2, 1）、順に、以下に示すステップS233～ステップS240を繰り返す。次に、公開簿生成部506は、ステップS233からステップS240において、階層番号mにより示される階層内の各ノードについて順に、以下に示すステップS234～ステップS239を繰り返す。

【0186】公開簿生成部506は、当該ノードに対応するノード情報をDVD用木構造テーブル511から読み出し（ステップS234）、読み出したノード情報をノード鍵M<sub>k</sub>を抽出する（ステップS235）。次に、公開簿生成部506は、当該ノードの直下に接続さ

れている2個の下位ノードのうち、右側の下位ノードのノード情報を、DVD用木構造テーブル511から読み出し（ステップS236）、次に、読み出したノード情報をノード鍵kを抽出する（ステップS237）。さらに、公開簿生成部506は、抽出したノード鍵kを鍵として用いて、ノード鍵M<sub>k</sub>に暗号化アルゴリズムE4を施して、暗号化ノード鍵E4（k, M<sub>k</sub>）を生成し（ステップS238）、当該ノードに対応するインデックス情報（階層番号、ノード番号）と暗号化ノード鍵E4（k, M<sub>k</sub>）とを、公開情報として、DVD用公開簿521へ書き込む（ステップS239）。

【0187】1.17 映画放送システム管理装置800の動作

映画放送システム管理装置800の動作について、図31～図33に示すフローチャートを用いて説明する。木構造構築部804は、映画放送用木構造テーブル811を生成して情報記憶部808へ書き込む（ステップS261）。

【0188】次に、制御部802は、鍵管理装置100から送受信部807を介して、機器ID及びシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>を受け取り、受け取った機器ID及びシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>を木構造構築部804へ出力する（ステップS262）。次に、木構造構築部804は、映画放送用木構造テーブル811において、受け取ったシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>が1個のリーフに対応するように、機器ID及びシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>を映画放送用木構造テーブル811に書き込む（ステップS263）。次に、制御部802は、送受信部807及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID（=3）とリーフ番号とを送信する（ステップS264）。

【0189】次に、制御部802は、機器ID及びシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>の受取りが終了したか否かを判断し、終了していないと判断する場合には（ステップS265）、ステップS262へ戻って処理を繰り返す。制御部802が、機器ID及びシステム用機器鍵S<sub>kdi</sub><sup>(3)</sup>の受取りが終了したと判断する場合には（ステップS265）、公開簿生成部806は、システムID（ここでは、「3」）を映画用公開簿821へ書き込み（ステップS266）、情報記憶部808から初期値x<sub>0</sub>を読み出し（ステップS267）、読み出した初期値x<sub>0</sub>を映画用公開簿821へ書き込む（ステップS268）。

【0190】次に、公開簿生成部806は、ステップS269からステップS281において、階層3から階層1まで（階層の番号m=3, 2, 1）順に、以下に示すステップS270～ステップS280を繰り返す。次に、公開簿生成部806は、ステップS270からステップS280において、階層番号mにより示される階層

内の各ノードについて順に、以下に示すステップS 27 1～ステップS 27 9を繰り返す。

【0191】公開簿生成部806は、当該ノードの下位に接続する2個の下位ノードに、それぞれ対応する2個のノード情報を映画放送用木構造テーブル811から読み出し（ステップS 27 1）、読み出した2個のノード情報からそれぞれ2個のノード鍵N k 1、N k 2を抽出する（ステップS 27 2）。次に、公開簿生成部806は、当該2個のノード鍵N k 1、N k 2をそれぞれ2個の点とみなし、2個の点を通る直線Lを求め（ステップS 27 3）、直線L上の点（x<sub>0</sub>、s<sub>(y)</sub>）を求め（ステップS 27 4）、公開点y座標s<sub>(y)</sub>を映画用公開簿821へ書き込む（ステップS 27 5）。次に、公開簿生成部806は、直線Lのy切片Y Iを求め（ステップS 27 6）、一方向性関数gを用いて、g（Y I）を算出し（ステップS 27 7）、g（Y I）をx座標とする直線L上の点のy座標Y Gを求め（ステップS 27 8）、求めた点（g（Y I）、Y G）をノード鍵とし、ノード鍵を当該ノードに対応付けて映画放送用木構造テーブル811へ書き込む（ステップS 28 0）。

【0192】ステップS 26 9からステップS 28 1における各階層についての繰り返しが終了すると、制御部802は、送受信部807を介して、生成した映画用公開簿821を、送信装置1000へ送信し、送信装置1000は、放送衛星6を介して、映画用公開簿821を放送波に載せて放送する（ステップS 28 2）。制御部802は、映画放送用木構造テーブル811から、1個のノード鍵を選択し（ステップS 28 3）、選択したノード鍵を、映画コンテンツ供給装置900へ送信する（ステップS 28 4）。

### 【0193】1. 18 利用者機器1100の動作

#### （1）利用者機器1100全体の動作

利用者機器1100全体の動作について、図34に示すフローチャートを用いて説明する。情報抽出部1108は、音楽配信システム管理装置200から、インターネット5及び送受信部1110を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「音楽配信システム」と対応付けて、システムIDテーブル1151へ書き込む。また、情報抽出部1108は、DVD供給システム管理装置500から、インターネット5及び送受信部1110を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「DVD供給システム」と対応付けて、システムIDテーブル1151へ書き込む。また、情報抽出部1108は、映画放送システム管理装置800から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、システムID及びリーフ番号を受信し、受信したシステムID及びリーフ番号をシステム名「映画放送システム」と対応付けて、システム

50 IDテーブル1151へ書き込む（ステップS 30 1）。

【0194】次に、情報抽出部1108は、公開簿サーバ装置400から、インターネット5及び送受信部1110を介して、音楽用公開簿を受信し、受信した音楽用公開簿を、音楽用公開簿1161として情報記憶部1101へ書き込む。また、利用者によりDVD用公開簿が記録されているDVDが利用者機器1100に装着されると、情報抽出部1108は、装着されたDVDから、DVD接続部1111を介して、DVD用公開簿を読み出し、読み出したDVD用公開簿を、DVD用公開簿1162として情報記憶部1101へ書き込む。また、情報抽出部1108は、映画放送システム管理装置800から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、映画用公開簿を受信し、受信した映画用公開簿を、映画用公開簿1163として情報記憶部1101へ書き込む（ステップS 30 2）。

【0195】次に、制御部1105は、利用者から入力部1106を介して、利用するシステム名の入力を受け付け（ステップS 30 3）、情報記憶部1101が有するシステムIDテーブル1151から、入力を受け付けたシステム名に対応するシステムIDを取得する（ステップS 30 4）。次に、情報抽出部1108は、音楽コンテンツ配信装置300から、インターネット5及び送受信部1110を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む。又は、利用者により暗号化グループ鍵及び暗号化コンテンツが記録されているDVDが利用者機器1100に装着されると、情報抽出部1108は、装着されたDVDから、DVD接続部1111を介して、暗号化グループ鍵及び暗号化コンテンツを読み出し、読み出した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む。又は、情報抽出部1108は、映画コンテンツ供給装置900から、送信装置1000、送信用アンテナ10、放送衛星6、受信用アンテナ9及びチューナ部1112を介して、暗号化グループ鍵及び暗号化コンテンツを受信し、受信した暗号化グループ鍵及び暗号化コンテンツを、暗号化グループ鍵1171及び暗号化コンテンツ1181として、情報記憶部1101へ書き込む（ステップS 30 5）。

【0196】次に、制御部1105は、システムIDが「1」、「2」又は「3」のいずれであるかを判断し、システムIDが「1」であると判断する場合に（ステップS 30 6）、ノード鍵特定部1103は、ノード鍵の特定（1）の処理を行う（ステップS 30 7）。システムIDが「2」であると判断する場合に（ステップS 3

0 6)、ノード鍵特定部 1103 は、ノード鍵の特定(2)の処理を行う(ステップ S 308)。システム ID が「3」であると判断する場合に(ステップ S 306)、ノード鍵特定部 1103 は、ノード鍵の特定(3)の処理を行う(ステップ S 309)。

【0197】ノード鍵特定部 1103 によるノード鍵の特定が終了すると、復号部 1104 は、情報記憶部 1101 から暗号化グループ鍵を読み出し、特定されたノード鍵を鍵として用いて、読み出した暗号化グループ鍵を復号して、グループ鍵 D3(ノード鍵、暗号化グループ鍵)を生成する(ステップ S 310)。次に、復号部 1109 は、暗号化コンテンツを情報記憶部 1101 から読み出し、生成されたグループ鍵を鍵として用いて、読み出した暗号化コンテンツを復号して、コンテンツ D2(グループ鍵、暗号化コンテンツ)を生成する(ステップ S 311)。

【0198】次に、再生部 1113 は、生成されたコンテンツを再生して出力する(ステップ S 312)。次に、制御部 1105 は、コンテンツの復号処理が終了したか否かを判断し、終了していないと判断する場合に(ステップ S 313)、ステップ S 303 へ戻って、処理を繰り返す。終了したと判断する場合に(ステップ S 313)、制御部 1105 は、利用者機器 1100 によるコンテンツの復号、再生を終了する。

#### 【0199】(2) ノード鍵の特定(1)の動作

ノード鍵特定部 1103 によるノード鍵の特定(1)の動作について、図 35～図 36 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 34 のフローチャートのステップ S 307 の詳細である。ノード鍵特定部 1103 は、情報記憶部 1101 が有するシステム ID テーブル 1151 から、システム ID に対応するリーフ番号を読み出し(ステップ S 321)、機器鍵記憶部 1102 から、機器鍵 kdi を読み出し(ステップ S 322)、システム ID に対応する公開簿を特定する。ここでは、システム ID は、「1」であるので、音楽用公開簿 1161 が特定される(ステップ S 323)。

【0200】次に、ノード鍵特定部 1103 は、システム用機器鍵  $S_{kdi}^{(1)} = h$ (kdi、システム ID)を生成し(ステップ S 324)、リーフ番号から階層 3 のパス番号を求め(ステップ S 325)、インデックス情報=(3、パス番号)を設定し(ステップ S 326)、音楽用公開簿 1161 から設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 327)、次に、システム用機器鍵  $S_{kdi}^{(1)}$  を鍵として用いて、読み出した暗号化ノード鍵を復号する。 $R_3 = D1(S_{kdi}^{(1)}, \text{暗号化ノード鍵})$ (ステップ S 328)。

【0201】次に、ノード鍵特定部 1103 は、リーフ番号から階層 2 のパス番号を求め(ステップ S 32

9)、インデックス情報=(2、パス番号)を設定し(ステップ S 330)、音楽用公開簿 1161 から設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 331)、 $R_3$  を鍵として用いて、読み出した暗号化ノード鍵を復号する。 $R_2 = D1(R_3, \text{暗号化ノード鍵})$ (ステップ S 332)。

【0202】次に、ノード鍵特定部 1103 は、インデックス情報=(1, 1)を設定し(ステップ S 333)、音楽用公開簿 1161 から設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 334)、 $R_2$  を鍵として用いて、読み出した暗号化ノード鍵を復号する。 $R_1 = D1(R_2, \text{暗号化ノード鍵})$ (ステップ S 335)。

【0203】次に、ノード鍵特定部 1103 は、 $S_{kdi}^{(1)}$ 、 $R_3$ 、 $R_2$ 、 $R_1$  のうちから 1 個のノード鍵を決定する(ステップ S 336)。

#### (3) ノード鍵の特定(2)の動作

ノード鍵特定部 1103 によるノード鍵の特定(2)の動作について、図 37～図 40 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 34 のフローチャートのステップ S 308 の詳細である。

【0204】ノード鍵特定部 1103 は、情報記憶部 1101 が有するシステム ID テーブル 1151 から、システム ID に対応するリーフ番号を読み出し(ステップ S 351)、機器鍵記憶部 1102 から、機器鍵 kdi を読み出し(ステップ S 352)、システム ID に対応する公開簿を特定する。ここでは、システム ID は、「2」であるので、DVD 用公開簿 1162 が特定される(ステップ S 353)。

【0205】次に、ノード鍵特定部 1103 は、システム用機器鍵  $S_{kdi}^{(2)} = h$ (kdi、システム ID)を生成する(ステップ S 354)。次に、ノード鍵特定部 1103 は、木構造 T200 の階層 4 から階層 3 へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する(ステップ S 355)左パスをたどると決定する場合に(ステップ S 356)、ノード鍵特定部 1103 は、 $R_3 = g(S_{kdi}^{(2)})$  を求める(ステップ S 357)。右パスをたどると決定する場合に(ステップ S 356)、ノード鍵特定部 1103 は、リーフ番号から階層 3 のノード番号を求め(ステップ S 358)、インデックス情報=(3、ノード番号)を設定し(ステップ S 359)、DVD 用公開簿 1162 から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 360)、読み出した暗号化ノード鍵を、 $S_{kdi}^{(2)}$  を鍵として用いて、復号する。 $R_3 = D4(S_{kdi}^{(2)}, \text{暗号化ノード鍵})$ (ステップ S 361)。

【0206】次に、ノード鍵特定部 1103 は、木構造 T200 の階層 3 から階層 2 へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する(ステップ S 362)。左パスをたどると決定する場合に(ステップ S 363)、ノード鍵特定部 1103 は、リーフ番号から階層 2 のノード番号を求め(ステップ S 364)、インデックス情報=(3、ノード番号)を設定し(ステップ S 365)、DVD 用公開簿 1162 から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 366)、読み出した暗号化ノード鍵を、 $S_{kdi}^{(2)}$  を鍵として用いて、復号する。 $R_3 = D4(S_{kdi}^{(2)}, \text{暗号化ノード鍵})$ (ステップ S 367)。

【0207】次に、ノード鍵特定部 1103 は、木構造 T200 の階層 2 から階層 1 へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する(ステップ S 368)。左パスをたどると決定する場合に(ステップ S 369)、ノード鍵特定部 1103 は、リーフ番号から階層 1 のノード番号を求め(ステップ S 370)、インデックス情報=(3、ノード番号)を設定し(ステップ S 371)、DVD 用公開簿 1162 から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップ S 372)、読み出した暗号化ノード鍵を、 $S_{kdi}^{(2)}$  を鍵として用いて、復号する。 $R_3 = D4(S_{kdi}^{(2)}, \text{暗号化ノード鍵})$ (ステップ S 373)。

PS 362)。左パスをたどると決定する場合に(ステップS 363)、ノード鍵特定部1103は、 $R_2 = g(R_3)$ を求める(ステップS 364)。右パスをたどると決定する場合に(ステップS 363)、ノード鍵特定部1103は、リーフ番号から階層2のノード番号を求め(ステップS 365)、インデックス情報=(2、ノード番号)を設定し(ステップS 366)、DVD用公開簿1162から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップS 367)、読み出した暗号化ノード鍵を、 $R_3$ を鍵として用いて、復号する。 $R_2 = D_4(R_3, \text{暗号化ノード鍵})$ (ステップS 368)。

【0207】次に、ノード鍵特定部1103は、木構造T200の階層2から階層1へ、左パスをたどるか、右パスをたどるかをリーフ番号により、決定する(ステップS 369)。左パスをたどると決定する場合に(ステップS 370)、ノード鍵特定部1103は、 $R_1 = g(R_2)$ を求める(ステップS 371)。右パスをたどると決定する場合に(ステップS 370)、ノード鍵特定部1103は、インデックス情報=(1, 1)を設定し(ステップS 372)、DVD用公開簿1162から、設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップS 373)、読み出した暗号化ノード鍵を、 $R_2$ を鍵として用いて、復号する。 $R_1 = D_4(R_2, \text{暗号化ノード鍵})$ (ステップS 374)。

【0208】次に、ノード鍵特定部1103は、 $S_{kdi}^{(2)}$ 、 $R_3$ 、 $R_2$ 、 $R_1$ のうちから1個のノード鍵を決定する(ステップS 375)。

#### (4) ノード鍵の特定(3)の動作

ノード鍵特定部1103によるノード鍵の特定(3)の動作について、図4.1～図4.3に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図3.4のフローチャートのステップS 309の詳細である。

【0209】ノード鍵特定部1103は、情報記憶部1101が有するシステムIDテーブル1151から、システムIDに対応するリーフ番号を読み出し(ステップS 391)、機器鍵記憶部1102から、機器鍵 $kdi$ を読み出し(ステップS 392)、システムIDに対応する公開簿を特定する。ここでは、システムIDは、「3」であるので、映画用公開簿1163が特定される(ステップS 393)。

【0210】次に、ノード鍵特定部1103は、システム用機器鍵 $S_{kdi}^{(3)} = h(kdi, \text{システムID})$ を生成し(ステップS 394)、映画用公開簿1163から初期値 $x_0$ を読み出す(ステップS 395)。次に、ノード鍵特定部1103は、リーフ番号から階層4の公開点のノード番号を求め(ステップS 396)、インデックス情報=(4、公開点のノード番号)を設定し(ステップS 397)、設定したインデックス情報に対

応する公開点y座標 $y_4$ を映画用公開簿1163から読み出し(ステップS 398)、機器鍵 $kdi$ と公開点 $(x_0, y_4)$ を通る直線 $L_4$ を求め(ステップS 399)、直線 $L_4$ のy切片 $YI_4$ を求め(ステップS 400)、 $g(YI_4)$ を求め(ステップS 401)、 $g(YI_4)$ をx座標とする直線 $L_4$ 上の点のy座標 $YG_4$ を求め、 $R_3 = (g(YI_4), YG_4)$ とする(ステップS 402)。

【0211】次に、ノード鍵特定部1103は、リーフ番号から階層3の公開点のノード番号を求め(ステップS 403)、インデックス情報=(3、公開点のノード番号)を設定し(ステップS 404)、設定したインデックス情報に対応する公開点y座標 $y_3$ を映画用公開簿1163から読み出し(ステップS 405)、求めた $R_3$ と公開点 $(x_0, y_3)$ を通る直線 $L_3$ を求め(ステップS 406)、直線 $L_3$ のy切片 $YI_3$ を求め(ステップS 407)、 $g(YI_3)$ を求め(ステップS 408)、 $g(YI_3)$ をx座標とする直線 $L_3$ 上の点のy座標 $YG_3$ を求め、 $R_2 = (g(YI_3), YG_3)$ とする(ステップS 409)。

【0212】次に、ノード鍵特定部1103は、リーフ番号から階層2の公開点のノード番号を求め(ステップS 410)、インデックス情報=(2、公開点のノード番号)を設定し(ステップS 411)、設定したインデックス情報に対応する公開点y座標 $y_2$ を映画用公開簿1163から読み出し(ステップS 412)、求めた $R_2$ と公開点 $(x_0, y_2)$ を通る直線 $L_2$ を求め(ステップS 413)、直線 $L_2$ のy切片 $YI_2$ を求め(ステップS 414)、 $g(YI_2)$ を求め(ステップS 415)、 $g(YI_2)$ をx座標とする直線 $L_2$ 上の点のy座標 $YG_2$ を求め、 $R_1 = (g(YI_2), YG_2)$ とする(ステップS 416)。

【0213】次に、ノード鍵特定部1103は、 $S_{kdi}^{(3)}$ 、 $R_3$ 、 $R_2$ 、 $R_1$ のうちから1個のノード鍵を決定する(ステップS 417)。

#### 2. その他の変形例

音楽配信システム管理装置200及び利用者機器1100の変形例である音楽配信システム管理装置200b及び利用者機器1100b(これらについては図示していない)について説明する。なお、ここでは、音楽配信システム管理装置200及び利用者機器1100との相違点を中心として説明する。

【0214】2. 1 音楽配信システム管理装置200bの構成

変形例としての音楽配信システム管理装置200bは、音楽配信システム管理装置200と同様に、音楽配信システム2において用いられる暗号化のための鍵を管理し、暗号化のためのノード鍵を音楽コンテンツ配信装置300へ出力し、また音楽用公開簿を公開簿サーバ装置400を介して、利用者機器1100bに公開する。し

かしながら、音楽配信システム管理装置200bは、上記の暗号化のための鍵の管理方法及び音楽用公開簿の作成方法において、音楽配信システム管理装置200と相違する。

【0215】音楽配信システム管理装置200bは、音楽配信システム管理装置200と同様に、表示部201b、制御部202b、入力部203b、木構造構築部204b、公開簿生成部206b、送受信部207b及び情報記憶部208bから構成されている。音楽配信システム管理装置200bは、音楽配信システム管理装置200と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、音楽配信システム管理装置200bは、その機能を達成する。

【0216】(1) 情報記憶部208b  
情報記憶部208bは、音楽配信用木構造テーブル211b及び音楽用公開簿221bを有している。音楽配信用木構造テーブル211bは、図44に一例として示す木構造T400に対応しており、木構造T400を表現するためのデータ構造を示している。

【0217】後述するように、木構造構築部204bにより、木構造T400を表現するためのデータ構造が音楽配信用木構造テーブル211bとして生成され、情報記憶部208bに書き込まれる。

(木構造T400) 木構造T400は、図44に示すように、階層1から階層4までの4階層からなる2分木である。木構造T400は、木構造T100と同様の構造を有しているので、詳細の説明は、省略する。

【0218】(音楽配信用木構造テーブル211b) 音楽配信用木構造テーブル211bは、図45に示すように、木構造T400に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T400を構成する各ノードにそれぞれ対応している。ルートに対応するノード情報は、階層番号、ノード番号及びノード鍵を含む。また、ルート及びリーフを除くノードに対応するノード情報は、階層番号、ノード番号、ノード鍵及びパス情報を含む。また、リーフに対応するノード情報は、階層番号、ノード番号、ノード鍵及び機器IDを含む。

【0219】階層番号、ノード番号、ノード鍵及び機器IDについては、上述した通りであるので、説明を省略する。パス情報は、対応する階層番号及びノード番号により示されるノードから、上位のノードへ至るパスに一意に割り当てられた情報であり、乱数を用いて生成されたものである。ここで、対応する階層番号及びノード番号とは、当該パス情報を含むノード情報に含まれる階層番号及びノード番号を指す。なお、パス情報は、当該パスに一意に割り当てられた番号であるとしてもよい。

【0220】(音楽用公開簿221b) 音楽用公開簿221bは、図46に示すように、システムID、公開

鍵、第1所定数個のパス公開情報及び第2所定数個のノード鍵公開情報を含んで構成されている。システムIDは、上述したとおりであって、コンテンツを供給したり配信したりするコンテンツ供給システムを識別するための識別子である。

【0221】公開鍵は、RSA公開鍵暗号方式に基づいて生成され、整数e及び整数nを含む。整数e及び整数nについては、後述する。前記第1所定数は、木構造T400において、木構造T400に含まれる各ノード(ルート及びリーフを除く)から上位のノードへ至るパスの数である。各パス公開情報は、インデックス情報及びパス情報を含み、インデックス情報は、階層番号及びパス番号を含む。階層番号、パス番号及びパス情報については、上述したとおりであるので、説明を省略する。

【0222】前記第2所定数は、木構造T400において、木構造T400に含まれる各リーフから上位のノードへ至るパスの数である。各ノード鍵公開情報は、インデックス情報及び暗号化ノード鍵を含み、インデックス情報は、階層番号及びパス番号を含む。階層番号及びパス番号については、上述したとおりであるので、説明を省略する。暗号化ノード鍵は、対応するノードに割り当てられたノード鍵に、対応するパス番号により示されるパスにより接続される下位ノードに割り当てられたノード鍵を鍵として、暗号化アルゴリズムE1を施して生成されたものである。

【0223】音楽用公開簿221bに含まれるパス公開情報の一例は、図46に示すように、(1, 1)及びP<sub>1</sub>を含む。ここで、(1, 1)は、階層番号が1であり、パス番号が1であることを示している。また、P<sub>1</sub>は、パス情報である。また、音楽用公開簿221bに含まれるノード鍵公開情報の一例は、図46に示すように、(3, 1)及びE1(Skd1<sup>(1)</sup>, KeyD<sup>(1)</sup>)を含む。ここで、(3, 1)は、階層番号が3であり、パス番号が1であることを示している。また、E1(Skd1<sup>(1)</sup>, KeyD<sup>(1)</sup>)は、Skd1<sup>(1)</sup>を鍵として用いて、KeyD<sup>(1)</sup>に暗号化アルゴリズムE1を施して得られる暗号文であることを示している。

【0224】(2) 木構造構築部204b  
木構造構築部204bは、音楽配信用木構造テーブル211bを生成して情報記憶部208へ書き込む。具体的には、木構造構築部204bは、木構造T400に含まれる各ノードについて、階層番号とノード番号とを含むノード情報を生成し、生成したノード情報を音楽配信用木構造テーブル211b内に書き込む。なお、この時点では、各ノード情報には、ノード鍵、機器ID及びパス情報は、含まれていない。

【0225】木構造構築部204bは、鍵管理装置100から、制御部202bを介して、機器ID及びシステム用機器鍵Skd1<sup>(1)</sup>を受け取り、音楽配信用木構造テーブル211bにおいて、受け取ったシステム用機器

鍵  $S_{kdi}^{(1)}$  が 1 個のリーフに対応するように、受け取った機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  を音楽配信用木構造テーブル 211b に書き込む。また、前記リーフを示すリーフ番号を制御部 202b へ出力する。

【0226】(3) 制御部 202b

制御部 202b は、機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  の受取りが終了するまで、機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  の受取りと、システム用機器鍵の音楽配信用木構造テーブル 211b への書き込みと、利用者機器へのリーフ番号の送信とを繰り返すように制御する。

【0227】次に、制御部 202b は、鍵管理装置 100 から送受信部 207b を介して、機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  を受け取り、受け取った機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  を木構造構築部 204b へ出力する。また、制御部 202b は、木構造構築部 204 からリーフ番号を受け取り、送受信部 207 及びインターネット 5 を介して、受け取った機器 ID により示される利用者機器へ、システム ID (=1) と受け取ったリーフ番号とを送信する。

【0228】さらに、制御部 202b は、音楽配信用木構造テーブル 211b から、所定の基準に基づいて、1 個のノード鍵を選択する。ここでは、一例として、リーフからルートへの経路上に存在する全てのノードのうち、最上位のノード即ちルートに割り当てられたノード鍵を選択する。次に、制御部 202b は、選択したノード鍵を、音楽コンテンツ配信装置 300 へ送信する。

【0229】(4) 公開簿生成部 206b

制御部 202b が、機器 ID 及びシステム用機器鍵  $S_{kdi}^{(1)}$  の受取りが終了したと判断する場合には、公開簿生成部 206b は、システム ID を音楽用公開簿 221b へ書き込む。次に、公開簿生成部 206b は、素数\*

$$(a-2) \text{ 新たなノード鍵} = E_6((d, n), (M_k (+) P_{I_a})) \\ = (M_k (+) P_{I_a})^d \bmod n$$

を算出する。

【0234】ここで、 $P_{I_a}$  は、当該ノードから、当該ノードの直下で左側に接続する下位ノードへのパスに対応するパス情報である。また、演算 (+) は、排他的論理※

$$(a-4) \text{ 新たなノード鍵} = E_6((d, n), (M_k (+) P_{I_b})) \\ = (M_k (+) P_{I_b})^d \bmod n$$

を算出する。

【0235】ここで、 $P_{I_b}$  は、当該ノードから、当該ノードの直下で右側に接続する下位ノードへのパスに対応するパス情報である。

(a-5) 新たに算出したノード鍵を、当該ノードの直下で右側に接続する下位ノードのノード情報（音楽配信用木構造テーブル 211b 内）へ書き込む。次に、公開簿生成部 206b は、階層 3 内の各ノードについて順に、以下に示す処理 (b-1) ~ (b-7) を繰り返す。

\*  $p$ 、素数  $q$  を求め、積  $n = p \times q$  を演算して整数  $n$  を求め、整数  $n$  と互いに素である整数  $e$  を求め、整数  $n$  及び整数  $e$  を公開鍵として音楽用公開簿 221b へ書き込む。

【0230】次に、公開簿生成部 206b は、整数  $L = LCM(p-1, q-1)$  を求める。ここで、LCM は、最小公倍数である。次に、 $L$  を法とする整数  $e$  の逆元  $d$  を求める。

$$d = e^{-1} \bmod L$$

10 ここで、整数  $n$  及び整数  $d$  は、秘密鍵である。

【0231】次に、公開簿生成部 206b は、階層 1 から階層 3 までの各パスについて、乱数を生成し、生成した乱数を用いて、パス情報を生成し、生成したパス情報を、階層番号及びノード番号に対応付けて、音楽配信用木構造テーブル 211b へ書き込む。また、公開簿生成部 206b は、インデックス情報（階層番号、パス番号）に対応付けて、生成した各パス情報を音楽用公開簿 221b へ書き込む。

20 【0232】次に、公開簿生成部 206b は、乱数を生成し、生成した乱数を元にしてルートに割り当てる鍵  $K_{e y A}^{(1)}$  を生成する。次に、生成した鍵  $K_{e y A}^{(1)}$  をルートに割り当てるために、（階層番号、ノード番号）=（1, 1）に対応付けて、生成した鍵  $K_{e y A}^{(1)}$  をノード鍵として音楽配信用木構造テーブル 211b へ書き込む。

【0233】次に、公開簿生成部 206b は、階層 1 から階層 2 への順に、さらに、各階層内の各ノードについて順に、以下に示す処理 (a-1) ~ (a-5) を繰り返す。

30 (a-1) 公開簿生成部 206b は、音楽配信用木構造テーブル 211b から当該ノードのノード情報を読み出し、読み出したノード情報をノード鍵を、ノード鍵  $M_k$  として、抽出する

$$(a-2) \text{ 新たなノード鍵} = E_6((d, n), (M_k (+) P_{I_a})) \\ = (M_k (+) P_{I_a})^d \bmod n$$

※ 理和を示す。

(a-3) 新たに算出したノード鍵を、当該ノードの直下で左側に接続する下位ノードのノード情報（音楽配信用木構造テーブル 211b 内）へ書き込む。

$$(a-4) \text{ 新たなノード鍵} = E_6((d, n), (M_k (+) P_{I_b})) \\ = (M_k (+) P_{I_b})^d \bmod n$$

す。

(b-1) 公開簿生成部 206b は、音楽配信用木構造テーブル 211b から当該ノードのノード情報を読み出し、読み出したノード情報をノード鍵を、ノード鍵  $M_k$  として、抽出する。

(b-2) 次に、公開簿生成部 206b は、当該ノードの直下で左側に接続する下位ノードのノード情報を、音楽配信用木構造テーブル 211b から読み出し、読み出したノード情報をノード鍵を、ノード鍵  $M_{k1}$  とし

て、抽出する。

(b-3) 暗号化ノード情報=E1 (Mk1, Mk) を算出する。

(b-4) インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿221bへ書き込む。

(b-5) 音楽配信用木構造テーブル211bから当該ノードの直下で右側に接続する下位ノードのノード情報を読み出し、読み出したノード情報からノード鍵を、ノード鍵Mk2として、抽出する。

(b-6) 暗号化ノード情報=E1 (Mk2, Mk) を算出する。

(b-7) インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿221bへ書き込む。

【0236】次に、公開簿生成部206bは、生成した音楽用公開簿221bを、公開簿サーバ装置400へ送信する。

#### (5) 送受信部207b

送受信部207bは、通信回線を介して、音楽コンテンツ配信装置300と接続され、また、インターネット5を介して、利用者機器1100bと接続されている。

【0237】送受信部207bは、制御部202と音楽コンテンツ配信装置300との間で情報の送受信を行う。また、送受信部207bは、制御部202bと利用者機器1100bとの間で情報の送受信を行う。

#### (6) 表示部201b及び入力部203b

表示部201bは、制御部202bの制御の元に各種の情報を表示する。また、入力部203bは、音楽配信システム管理装置200bの管理者からの情報の入力を受け付ける。

#### 【0238】2.2 利用者機器1100bの構成

変形例としての利用者機器1100bは、利用者機器1100と同様に、自身が記憶している機器鍵kdi及び音楽用公開簿に基づいて、暗号化音楽コンテンツを復号して、音楽コンテンツを再生し、自身が記憶している機器鍵kdi及びDVD用公開簿に基づいて、DVDに記録されている暗号化映画コンテンツを復号して、映画コンテンツを再生し、放送波を受信し、受信した放送波から暗号化映画コンテンツを抽出し、自身が記憶している機器鍵kdi及び映画用公開簿に基づいて、抽出した暗号化映画コンテンツを復号して、映画コンテンツを再生する。しかしながら、利用者機器1100bは、自分が記憶している機器鍵kdi及び音楽用公開簿に基づいて、自身のために割り当てられた鍵を特定する方法において、利用者機器1100と相違する。

【0239】利用者機器1100bは、利用者機器1100と同様の構成を有している。ここでは、利用者機器1100との相違点を中心として説明する。

#### (1) ノード鍵特定部1103

ノード鍵特定部1103は、情報記憶部1101が有するシステムIDテーブル1151から、システムIDに

対応するリーフ番号を読み出し、機器鍵記憶部1102から、機器鍵kdiを読み出す。また、システムIDに対応する公開簿を特定する。ここでは、システムIDは、「1」であるので、音楽用公開簿1161が特定される。

【0240】次に、ノード鍵特定部1103は、システム用機器鍵Skdi<sup>(1)</sup>=h (kdi、システムID)を生成する。こうして、階層4のノードに割り当てられたノード鍵Skdi<sup>(1)</sup>が求められる。次に、ノード鍵特定部1103は、階層3のノードに割り当てられたノード鍵を次に示すようにして、取得する。ノード鍵特定部1103は、リーフ番号から階層3のパス番号を求め、インデックス情報=(3、パス番号)を設定し、音楽用公開簿1161から設定したインデックス情報に対応する暗号化ノード鍵を読み出し、次に、システム用機器鍵Skdi<sup>(1)</sup>を鍵として用いて、読み出した暗号化ノード鍵を復号する。R<sub>3</sub>=D1 (Skdi<sup>(1)</sup>、暗号化ノード鍵)。こうして、階層3のノードに割り当てられたノード鍵R<sub>3</sub>が求められる。

【0241】次に、ノード鍵特定部1103は、階層2～1のノードに割り当てられたノード鍵を次に示すようにして、取得する。ノード鍵特定部1103は、音楽用公開簿1161から公開鍵e、nを読み出し、R<sub>2</sub>=D6 ((e, n), R<sub>3</sub>)=(R<sub>3</sub>)<sup>e</sup> mod nを算出する。次に、ノード鍵特定部1103は、リーフ番号から階層2のパス番号を求め、インデックス情報=(2、パス番号)を設定し、音楽用公開簿1161から設定したインデックス情報に対応するパス情報を、パス情報PIとして、読み出し、R<sub>2</sub>=R<sub>2</sub> (+) PIを算出する。こうして、階層2のノードに割り当てられたノード鍵R<sub>2</sub>が求められる。

【0242】次に、ノード鍵特定部1103は、R<sub>1</sub>=D6 ((e, n), R<sub>2</sub>)=(R<sub>2</sub>)<sup>e</sup> mod nを算出する。次に、ノード鍵特定部1103は、リーフ番号から階層1のパス番号を求め、インデックス情報=(1、パス番号)を設定し、音楽用公開簿1161から設定したインデックス情報に対応するパス情報を、パス情報PIとして、読み出し、R<sub>1</sub>=R<sub>1</sub> (+) PIを算出する。こうして、階層2のノードに割り当てられたノード鍵R<sub>1</sub>が求められる。

【0243】次に、ノード鍵特定部1103は、Skdi<sup>(1)</sup>、R<sub>3</sub>、R<sub>2</sub>、R<sub>1</sub>のうちから1個のノード鍵を決定する。

#### 2.3 音楽配信システム管理装置200bの動作

音楽配信システム管理装置200bの動作について、図47～図51に示すフローチャートを用いて説明する。

【0244】木構造構築部204bは、音楽配信用木構造テーブル211bを生成して情報記憶部208bへ書き込む(ステップS431)。次に、制御部202bは、鍵管理装置100から送受信部207bを介して、

機器ID及びシステム用機器鍵 $S_{kdi}^{(1)}$ を受け取り、受け取った機器ID及びシステム用機器鍵 $S_{kdi}^{(1)}$ を木構造構築部204bへ出力する(ステップS432)。次に、木構造構築部204bは、音楽配信用木構造テーブル211bにおいて、受け取ったシステム用機器鍵 $S_{kdi}^{(1)}$ が1個のリーフに対応するように、機器ID及びシステム用機器鍵 $S_{kdi}^{(1)}$ を音楽配信用木構造テーブル211bに書き込む(ステップS433)。次に、制御部202bは、送受信部207b及びインターネット5を介して、受け取った機器IDにより示される利用者機器へ、システムID(=1)とリーフ番号とを送信する(ステップS434)。

【0245】次に、制御部202bは、機器ID及びシステム用機器鍵 $S_{kdi}^{(1)}$ の受取りが終了したか否かを判断し、終了していないと判断する場合には(ステップS436)、ステップS432へ戻って処理を繰り返す。制御部202bが、機器ID及びシステム用機器鍵 $S_{kdi}^{(1)}$ の受取りが終了したと判断する場合には(ステップS436)、さらに、公開簿生成部206bは、システムIDを音楽用公開簿221bへ書き込む(ステップS437)。

【0246】次に、公開簿生成部206bは、素数p、素数qを求め(ステップS438)、積n=p×qを演算して整数nを求め(ステップS439)、整数nと互いに素である整数eを求め(ステップS440)、整数n及び整数eを公開鍵として音楽用公開簿221bへ書き込む(ステップS441)。次に、公開簿生成部206bは、整数L=L CM(p-1, q-1)を求める。ここで、L CMは、最小公倍数である(ステップS442)。次に、Lを法とする整数dの逆元dを求める。d =  $e^{-1} \bmod L$ (ステップS443)。

【0247】次に、公開簿生成部206bは、階層1から階層3までの各パスについて、パス情報を生成し、生成したパス情報を、階層番号及びノード番号に対応付けて、音楽配信用木構造テーブル211bへ書き込み(ステップS444)、インデックス情報(階層番号、パス番号)に対応付けて、生成した各パス情報を音楽用公開簿221bへ書き込む(ステップS445)。

【0248】次に、公開簿生成部206bは、乱数を生成し、生成した乱数を元にしてルートに割り当てる鍵 $K_{eyA}^{(1)}$ を生成し、生成した鍵 $K_{eyA}^{(1)}$ をルートに割り当てるために、(階層番号、ノード番号)=(1, 1)に対応付けて、鍵 $K_{eyA}^{(1)}$ をノード鍵として音楽配信用木構造テーブル211bへ書き込む(ステップS446)。

【0249】次に、公開簿生成部206bは、ステップS447からステップS456において、階層1から階層2まで(階層の番号m=1, 2)、順に、以下に示すステップS448～ステップS455を繰り返す。次に、公開簿生成部206bは、ステップS448からス

テップS455において、階層番号mにより示される階層内の各ノードについて順に、以下に示すステップS449～ステップS454を繰り返す。

【0250】公開簿生成部206bは、音楽配信用木構造テーブル211bから当該ノードのノード情報を読み出し(ステップS449)、読み出したノード情報からノード鍵を、ノード鍵Mkとして、抽出する(ステップS450)。次に、新たなノード鍵=E6((d, n)、(Mk (+) PIa))=(Mk (+) PIa) $^d \bmod n$ を算出し(ステップS451)、新たに算出したノード鍵を、当該ノードの直下で左側に接続する下位ノードのノード情報(音楽配信用木構造テーブル211b内の)へ書き込む(ステップS452)。さらに、新たなノード鍵=E6((d, n)、(Mk (+) PIb))=(Mk (+) PIb) $^d \bmod n$ を算出し(ステップS453)、新たに算出したノード鍵を、当該ノードの直下で右側に接続する下位ノードのノード情報(音楽配信用木構造テーブル211b内の)へ書き込む(ステップS454)。

【0251】次に、公開簿生成部206bは、ステップS457からステップS468において、階層3内の各ノードについて順に、以下に示すステップS458～ステップS467を繰り返す。公開簿生成部206bは、音楽配信用木構造テーブル211bから当該ノードのノード情報を読み出し(ステップS458)、読み出したノード情報からノード鍵を、ノード鍵Mkとして、抽出する(ステップS459)。

【0252】次に、公開簿生成部206bは、当該ノードの直下で左側に接続する下位ノードのノード情報を、音楽配信用木構造テーブル211bから読み出し(ステップS460)、読み出したノード情報からノード鍵を、ノード鍵Mk1として、抽出し(ステップS461)、暗号化ノード情報=E1(Mk1, Mk)を算出し(ステップS462)、インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿221bへ書き込む(ステップS463)。

【0253】次に、音楽配信用木構造テーブル211bから当該ノードの直下で右側に接続する下位ノードのノード情報を読み出し(ステップS464)、読み出したノード情報からノード鍵を、ノード鍵Mk2として、抽出し(ステップS465)、暗号化ノード情報=E1(Mk2, Mk)を算出し(ステップS466)、インデックス情報とともに、算出した暗号化ノード情報を音楽用公開簿221bへ書き込む(ステップS467)。

【0254】次に、公開簿生成部206bは、生成した音楽用公開簿221bを、公開簿サーバ装置400へ送信し(ステップS469)、制御部202bは、音楽配信用木構造テーブル211bから、1個のノード鍵を選択し(ステップS470)、選択したノード鍵を、音楽コンテンツ配信装置300へ送信する(ステップS47

1)。

**【0255】2.4 利用者機器1100bの動作**  
利用者機器1100bの動作のうち、ノード鍵特定部1103bによるノード鍵の特定(1)の動作について、図52～図53に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図34のフローチャートのステップS307の詳細である。

**【0256】ノード鍵特定部1103bは、情報記憶部1101bが有するシステムIDテーブル1151から、システムIDに対応するリーフ番号を読み出し(ステップS491)、機器鍵記憶部1102bから、機器鍵 $S_{kdi}^{(1)}$ を読み出し(ステップS492)、システムIDに対応する公開簿を特定する。ここでは、システムIDは、「1」であるので、音楽用公開簿1161が特定される(ステップS493)。**

**【0257】**次に、ノード鍵特定部1103bは、システム用機器鍵 $S_{kdi}^{(1)} = h(kdi)$ 、システムIDを生成し(ステップS494)、リーフ番号から階層3のパス番号を求め(ステップS495)、インデックス情報=(3、パス番号)を設定し(ステップS496)、音楽用公開簿1161から設定したインデックス情報に対応する暗号化ノード鍵を読み出し(ステップS497)、次に、システム用機器鍵 $S_{kdi}^{(1)}$ を鍵として用いて、読み出した暗号化ノード鍵を復号する。 $R_3 = D1(S_{kdi}^{(1)}, \text{暗号化ノード鍵})$ (ステップS498)。

**【0258】**次に、ノード鍵特定部1103bは、音楽用公開簿1161から公開鍵e、nを読み出し(ステップS499)、 $R_2 = D6((e, n), R_3) = (R_3)^e \bmod n$ を算出する(ステップS500)。次に、ノード鍵特定部1103bは、リーフ番号から階層2のパス番号を求め(ステップS501)、インデックス情報=(2、パス番号)を設定し(ステップS502)、音楽用公開簿1161から設定したインデックス情報に対応するパス情報を、パス情報PIとして、読み出し(ステップS503)、 $R_2 = R_2 (+) PI$ を算出する(ステップS504)、 $R_1 = D6((e, n), R_2) = (R_2)^e \bmod n$ を算出する(ステップS505)。

**【0259】**次に、ノード鍵特定部1103bは、リーフ番号から階層1のパス番号を求め(ステップS506)、インデックス情報=(1、パス番号)を設定し(ステップS507)、音楽用公開簿1161から設定したインデックス情報に対応するパス情報を、パス情報PIとして、読み出し(ステップS508)、 $R_1 = R_1 (+) PI$ を算出する(ステップS509)。

**【0260】**次に、ノード鍵特定部1103bは、 $S_{kdi}^{(1)}$ 、 $R_3$ 、 $R_2$ 、 $R_1$ のうちから1個のノード鍵を決定する(ステップS510)。

3.まとめ

### 3.1 本発明の概要

以上説明したように、本発明は、1個の利用者機器が、異なる複数のコンテンツ配信システムに接続され、各コンテンツ配信システムからコンテンツの配信サービスの提供を受ける際に、それぞれのコンテンツ配信システムにおいて、柔軟でかつそれぞれ独自の木構造を用いてグループ鍵の管理を行うことができる暗号化伝送システムに関する。

**【0261】**各利用者機器は、木構造のリーフに対応した機器鍵を保持しており、機器鍵とシステム毎に公開されている公開簿を用いて、リーフから順次上位に木構造を再構成し、各利用者機器に対応するノード鍵を求め、求めたノード鍵に基づいて、暗号化コンテンツを復号する。公開簿は、それぞれのシステムが提供するWebサーバ、DVDなどのパッケージメディア、デジタル放送により各利用者機器に対して公開される。

**【0262】**鍵管理機関により管理運営される鍵管理装置は、機器鍵を安全に保存すると共に、機器鍵を対応する利用者機器に配布する。また、コンテンツ供給システムのシステム管理者に対し、システム用機器鍵を配布する。ここで、システム用機器鍵は、機器鍵を当該コンテンツ供給システム用に変換した鍵である。コンテンツ供給システムのシステム管理装置は、システム用機器鍵を用いて、木構造を構築し公開簿を生成し、これを管理する。また、コンテンツ供給システムのコンテンツ供給者に対して、グループ鍵を暗号化するために必要となる各ノード鍵を指定する。

**【0263】**コンテンツ供給システムのコンテンツ供給装置は、各利用者機器に対し、コンテンツ供給システム固有のコンテンツサービスを提供する。コンテンツ供給装置は、コンテンツに対応してグループ鍵を生成し、グループ鍵をシステム管理装置から受け取ったノード鍵を用いて暗号化して、暗号化鍵情報(グループ鍵を特定の利用者機器で求めるための鍵情報)を生成し、グループ鍵を用いて暗号化されたコンテンツとともに、各利用者機器に配布する。

**【0264】**各利用者機器は、予め鍵管理装置から配布された固定で個別の機器鍵を有し、機器鍵を用いて、各利用者機器が加入しているコンテンツ供給システムのためのシステム用機器鍵を生成し、コンテンツ供給装置から供給される暗号化鍵情報及び暗号化コンテンツを受信する。ここで、各利用者機器に関して、次のように仮定する。

**【0265】(a)**各利用者機器が有している機器鍵は変更されない。機器鍵は、例えば、製造時に埋め込まれるものとする。

**(b)**各利用者機器は、異なる複数のコンテンツ供給システムに加入可能であり、それぞれのコンテンツ供給システムにより提供されるコンテンツサービスを受けることができる。

【0266】(c) 各利用者機器は、デジタル放送、ホームページ、パッケージメディアなどにより、公開される公開簿にアクセス可能である。

### 3.2 運用手順の例

次に、運用手順の例について説明する。

#### <1>利用者機器の製造時

ここで、利用者機器のIDを*i*とする。

【0267】鍵管理装置は、対応する利用者機器*i*の機器鍵k<sub>d i</sub>を生成し、安全に保管すると共に、製造業者を介して、利用者機器*i*の製造時に、機器鍵k<sub>d i</sub>を利用者機器*i*に埋め込む。

#### <2>コンテンツ供給システムの立上げ時

コンテンツ供給システムのIDをID1とする。

【0268】(1) 鍵管理装置は、コンテンツ供給システムのIDを用いて、システム用の機器*i*の鍵h (k<sub>d i</sub>, ID1)を求める。ここでhは、公開の一方向性関数とする。システム用の機器鍵の生成に一方向性関数を用いることにより、コンテンツ供給システムのシステム管理者は、システム用の機器鍵から機器の鍵自身k<sub>d i</sub>を求ることもできないし、また、他のコンテンツ供給システム用の機器鍵を求ることもできない。

【0269】(2) 鍵管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵をコンテンツ供給システムのシステム管理者が管理、運営するシステム管理装置へ秘密に渡す。

(3) システム管理装置は、任意にグループ鍵を管理するための木構造を構築し、さらに、システム用機器鍵を用いて公開簿を生成する。

【0270】(4) システム管理装置は、生成した公開簿を、例えば、デジタル放送、Webサーバや、パッケージメディアを用いて、利用者機器に対して公開する。

#### <3>コンテンツ配布時

(1) システム管理装置は、コンテンツを渡す相手の利用者機器を管理し、コンテンツを暗号化するために使用する木構造のノード鍵を選択する。システム管理装置は、選んだノード鍵（デバイス鍵と称することもある）を、コンテンツ供給装置へ配布する。コンテンツは、選ばれたノード鍵（デバイス鍵）に基づいて、暗号化される。なお、ここでは、システム管理装置が、コンテンツを暗号化する際に基づくノード鍵の選択を行うものとしているが、コンテンツ供給装置が行うとしてもよい。

【0271】(2) コンテンツ供給装置は、任意のグループ鍵を生成し、生成したグループ鍵をシステム管理装置により指定されたノード鍵を用いて暗号化し、その結果を暗号化鍵情報とし、暗号化鍵情報と、グループ鍵を用いて暗号化されたコンテンツとともに、例えば、インターネット、DVDなどのパッケージメディアや、放送メディアを用いて利用者機器に供給する。

【0272】(3) 利用者機器は、自身の機器鍵k<sub>d i</sub>とコンテンツ供給システムのIDを用いて、コンテンツ

供給システム用の機器鍵h (k<sub>d i</sub>, ID1)を求める。

(4) 利用者機器は、システム用の機器鍵と公開簿を用いてコンテンツ供給システムの木構造における自身のノード鍵を順次求める。

(5) 利用者機器は、コンテンツ供給装置から供給された暗号化鍵情報から自身に対応する暗号文を選び、ノード鍵を用いて復号してグループ鍵を求め、さらにグループ鍵を用いてコンテンツを求める。

10 【0273】ここまでにおいて、1個のコンテンツ供給システムの場合のみについて説明してきたが、さらに、別のコンテンツ供給システムシステムが追加される場合も、前記コンテンツ供給システムの立上げおよび運用と同様に行えばよい。このとき、利用者機器*i*は、公開の一方向性関数とシステムのIDを用いて、内部で新たなコンテンツ供給システム用の機器鍵を生成するだけでも、例えば、ICカードなどの別途の方法を用いて利用者機器に秘密鍵等を追加する必要はない。

【0274】次に、上記の公開簿の生成方法、及び利用者機器において機器鍵からコンテンツを復号するため必要なノード鍵の求め方について、4つの具体例を述べる。なお、例として、コンテンツ供給システムが、3階層の木構造分割方法に対応した公開簿を生成する場合について述べる。各利用者機器*i*は、機器鍵のみを保持し、機器鍵より一方向性関数を用いてシステム用機器鍵S<sub>k d i</sub><sup>(1)</sup> (= h (k<sub>d i</sub>, ID1))を求める。また各利用者機器*i*は、公開簿を用いて木構造における対応するノード鍵を求める。また、h、gを公開の一方向性関数とする。

30 【0275】<4>具体例1=共通鍵暗号を利用した方法

具体例1は、音楽配信システム2において説明したものに対応する。

#### (1) システム管理装置による木構造の決定

システム管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵S<sub>k d 1</sub><sup>(1)</sup> ~ S<sub>k d 8</sub><sup>(1)</sup>を木構造のリーフに割り当て、図6に示す木構造の各ノード鍵を任意に決める。

【0276】(2) システム管理装置による公開簿の生成

システム管理装置は、木構造の各パスに対応した暗号文を生成する。例えば、利用者機器1のリーフからK<sub>e y D</sub><sup>(1)</sup>が割り当てられたノードへのパスに対応して、コンテンツ供給システム用の機器鍵S<sub>k d 1</sub><sup>(1)</sup>を鍵として用いて、K<sub>e y D</sub><sup>(1)</sup>を暗号化して、暗号文E<sub>1</sub> (S<sub>k d 1</sub><sup>(1)</sup>, K<sub>e y D</sub><sup>(1)</sup>)を求める。なお、暗号化アルゴリズムE<sub>1</sub>は、例えば、DESやAESなどの共通鍵暗号とし、これに対応する復号アルゴリズムD<sub>1</sub>は公開されているものとする。

50 【0277】また、機器2のリーフからK<sub>e y D</sub><sup>(1)</sup>が

割り当てられたノードへのパスに対応しては、E 1 (S k d 2<sup>(1)</sup>、Key D<sup>(1)</sup>) を求める。以下同様に求めて、これらを図8に示す公開簿に公開する。なお、公開簿には暗号文とともに、その暗号文がどのパスに対応した暗号文なのかを示すインデックス情報を載せる。インデックス情報の例としては、木構造の階層番号とその階層における左からの番号とを用いることができる。暗号文 E 1 (k d 1<sup>(1)</sup>、Key D<sup>(1)</sup>) のインデックス情報としては、例えば、上位から 3 層目の最も左のパスであることより、(3, 1) を付加する。以下同様である。

【0278】(3) 各利用者機器によるノード鍵の算出  
各利用者機器は、システム用の機器鍵から、上記公開簿を用いて順次木構造を上にたどり、ノード鍵を求める。例えば、機器 ID が「1001」である利用者機器 1 は、まず、自身の機器鍵 k d 1 とシステム 1 の ID 番号を一方向性関数 h の入力として、コンテンツ供給システム用の機器鍵 S k d 1<sup>(1)</sup> を求める。そして、公開簿から E 1 (S k d 1<sup>(1)</sup>、Key D<sup>(1)</sup>) を取り出して、これを復号して、1つ上の層のノード鍵 Key D<sup>(1)</sup> を求める。さらに、E 1 (Key D<sup>(1)</sup>、Key B<sup>(1)</sup>) を復号して、さらに、上位層のノード鍵 Key B<sup>(1)</sup> を求める。最後に、E 1 (Key B<sup>(1)</sup>、Key A<sup>(1)</sup>) を復号して、ルートの Key A<sup>(1)</sup> を求める。なお、公開簿から所望の暗号文を取り出すには、予め機器内に埋め込まれている木構造における自身の位置情報とインデックス情報を用いる。なお、利用者機器が上記獲得したノード鍵のうちどれを用いて、コンテンツ供給者から供給されたコンテンツを復号するのかについては、従来どおりコンテンツに付随して供給される暗号化鍵情報を用いる。

【0279】<5>具体例 2 = 一方向性関数を利用した方法

具体例 2 は、DVD 供給システム 3 において説明したものに対応する。具体例 2 は、具体例 1 における各ノードの左パスに一方向性関数を用いることにより、公開簿のデータ容量を削減している。

#### (1) システム管理装置による木構造の決定

システム管理装置は、コンテンツ供給システムに加入する利用者機器のシステム用機器鍵 S k d 1<sup>(2)</sup> ~ S k d 8<sup>(2)</sup> を、図 13 に示す木構造のリーフに割り当てる。

【0280】(2) システム管理装置による公開簿の生成

システム管理装置は、一方向性関数 g を用いて、g (S k d 1<sup>(2)</sup>)、g (S k d 3<sup>(2)</sup>)、g (S k d 5<sup>(2)</sup>)、g (S k d 7<sup>(2)</sup>) をそれぞれ求めて、リーフの1つ上の層のノード鍵 Key D<sup>(2)</sup>、Key E<sup>(2)</sup>、Key F<sup>(2)</sup>、Key G<sup>(2)</sup> とする。

【0281】システム管理装置者は、公開簿に、E 4 (S k d 2<sup>(2)</sup>、Key D<sup>(2)</sup>)、E 4 (S k d

4<sup>(2)</sup>、Key E<sup>(2)</sup>)、E 4 (S k d 6<sup>(2)</sup>、Key F<sup>(2)</sup>)、E 4 (S k d 8<sup>(2)</sup>、Key G<sup>(2)</sup>) を登録する。なお、ここで例えば E 4 (S k d 2<sup>(2)</sup>、Key D<sup>(2)</sup>) は、S k d 2<sup>(2)</sup> を鍵としてノード鍵 Key D<sup>(2)</sup> を共通鍵暗号化して生成した暗号文である。

【0282】同様に、順次木構造の左パスは一方向性関数 g で上の層の鍵を求め、右パス用の暗号文を公開簿に登録する。結果として図 14 に示す公開簿を生成して、公開する。

#### (3) 各利用者機器によるノード鍵の算出

リーフに対応した機器鍵を保持する各利用者機器は、まず一方向性関数 h を用いてシステム用機器鍵を求める。次に、木構造における左パスを上位層にたどるときは一方向性関数 g を用い（図 13 において、実線で表す）、右パスをたどるときは公開簿の対応する暗号文を復号して（図 13 において、二重線で表す）、順次ルートに至るまでのノード鍵を求める。

【0283】例えば、機器 ID が「1003」である利用者機器 3 は、まず一方向性関数 g を用いて Key E<sup>(2)</sup> を求め、次に公開簿から E 4 (Key E<sup>(2)</sup>、Key B<sup>(2)</sup>) を復号して Key B<sup>(2)</sup> を求める。さらに、g を用いて Key A<sup>(2)</sup> を求める。なお、この例では左パスを一方向性関数を用いてたどるとしたが、層ごとに一方向性関数を用いるパスを変えてよい。また、ここでは同じ一方向性関数を用いているが、層ごとに異なる関数を用いても良い。一方向性関数を用いてたどるのか、公開簿を用いてたどるのか、あるいはどの一方向性関数を用いるのかの判断は、具体例 1 と同様に木構造における当該機器の位置と公開簿内の暗号文に付加するインデックス情報を用いればよい。

【0284】<6>具体例 3 = 密码分散のテクニックを利用した方法

具体例 3 は、映画放送システム 4 において説明したものに対応する。具体例 3 は、下位ノード鍵から共通の曲線（次数が 1 の場合は直線）を求めて、曲線から一意に決定される点を上位のノード鍵とする。この方法は密码分散と同様のテクニックである。なお、以下の曲線は、（以下特に説明はしないが）ある体上で求められるものとする。

40 【0285】(1) システム管理装置による木構造の決定

システム管理装置は、システムに加入する利用者機器のシステム用機器鍵 S k d 1<sup>(3)</sup> ~ S k d 8<sup>(3)</sup> を、図 16 に示す木構造のリーフに割り当てる。木構造のリーフにあたる機器鍵を、(x, y) 平面上の点とする。

#### (2) システム管理装置による木構造と公開簿の生成

システム管理装置は、S k d 1<sup>(3)</sup> 及び S k d 2<sup>(3)</sup> を通る直線を求めて、直線上の点を s 1 として公開する。s 1 の x 座標を予め決めておき、これを公開簿に載せて（ここでは x<sub>0</sub> とする）、s 1 の y 座標 s 1<sub>(y)</sub> だけを

公開簿に登録する。

【0286】直線からある決められた手順で同じ直線上の  $Key D^{(3)}$  を求める。なお、直線を求める人だけが  $Key D^{(3)}$  を求めることができるようとする。そのためには、例えば、この手順の中に一方向性関数  $g$  を含めればよい。例えば図18に示す例では、直線の切片  $y$  を一方向性関数で変換し、この値  $g(y)$  を  $x$  座標とする直線上の点を  $Key D^{(3)}$  としている。一方向性関数を用いることにより、利用者機器1と利用者機器2以外の利用者機器は、 $Key D^{(3)}$  の  $x$  座標を求めることがでない。

【0287】システム管理装置は、 $Key D^{(3)}$ 、 $Key E^{(3)}$  を通る直線を求め、直線上の点の  $y$  座標を  $s_5^{(9)}$  として公開し、 $Key B^{(3)}$  を求める。利用者機器1～利用者機器4は、 $Key D^{(3)}$  及び  $Key E^{(3)}$  を通る直線を求めることができるが、上記の理由により、利用者機器3と利用者機器4は、この直線より、 $Key D^{(3)}$  を求めることが困難である。

【0288】以下同様に、順次2つのノード鍵からその共通の上位ノード鍵と、公開簿への登録値を順次求める。公開簿への登録値を図20に示す。ここでの各登録値は、 $Skd1^{(3)}$ 、 $Skd2^{(3)}$  と公開値  $s_1$  および上位のノード鍵  $Key D$  の関係を、図19のように標記したときの、図16に示した点  $s_1 \sim s_7$  の  $y$  座標である。

【0289】(3) 各利用者機器によるノード鍵の算出  
各利用者機器は、自身の機器鍵と公開簿に登録されている値(双方とも(x, y)平面上の点)を通る直線を求め、順次上位の階層のノード鍵を求める。例えば、利用者機器1はまずシステム用機器鍵を求め、これと  $s_1$  を通る直線より  $Key D^{(3)}$  を求める。次に  $Key D^{(3)}$  と  $s_5$  を通る直線より  $Key B^{(3)}$  を求め、同様に順次、 $Key A^{(3)}$  を求める。

【0290】なお、この例では2進木の場合を述べたが、例えば3進木の場合はある親ノードから派生する3つのノードのノード鍵3点を通る2次曲線を求め、この上の任意の2点を公開簿に掲載する。利用者機器は自分が保持するノード鍵1点と、公開簿の2点より上記2次曲線を求め、1つ上のノード鍵を求める。

<7>具体例4=RSAを利用した方法

具体例4は、音楽配信システム2の変形例として説明したものに対応する。

【0291】(1) システム管理装置による木構造の決定

システム管理装置は、システムに加入する機器のシステム用機器鍵  $Skd1^{(1)} \sim Skd8^{(1)}$  を、図44に示す木構造のリーフに割り当てる。

(2) システム管理装置による木構造と公開簿の生成  
RSA暗号と同様に、素数  $p$ 、 $q$  を求めその積  $n = p \times q$  を公開する。 $n$  と互いに素な  $e$  を求めて公開すると共

に、 $L (=LCM(p-1, q-1))$  : LCMは最小公倍数)を法とした  $e$  の逆元  $d (=e^{-1} \bmod L : d$  は、秘密鍵)を求める。システム管理装置は、例えば図44に示すように各パスに対応したパス情報を決定し公開する。任意にルートの鍵  $Key A^{(1)}$  を求め、 $Key A^{(1)}$  と(左のパスの)パス情報  $p_1$  の排他的論理和を求めて、これを秘密鍵  $d$  を用いて暗号化した結果を  $Key B^{(1)}$  とする。また、 $Key A^{(1)}$  と(右のパスの)パス情報  $p_2$  の排他的論理和を求めて、これを  $d$  で暗号化した結果を  $Key C^{(1)}$  とする。以下同様にリーフの1つ上の層のノード鍵まで求める。以上で生成した公開簿を図46に示す。

【0292】最後の1層については、具体例1、具体例2、又は具体例3の方法を用いて、対応する公開簿を生成する。

(3) 各利用者機器によるノード鍵の算出

利用者機器は、具体例1、具体例2、又は具体例3の方法を用いて1つ上の層のノード鍵を求める。例えば、利用者機器1は、 $Key D^{(1)}$  を求める。次に、 $Key D^{(1)}$  を公開鍵  $e$  で復号し、その結果とパス情報  $p_3$  の排他的論理和を求めて上位層のノード鍵  $Key B^{(1)}$  を求める。さらに、 $Key B^{(1)}$  を公開鍵  $e$  で復号し、その結果とパス情報  $p_1$  との排他的論理和を求めてルートの鍵  $Key A^{(1)}$  を求める。

【0293】4. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

30 (1) 暗号化データ配信システム1において、3個のコンテンツ供給システムが含まれているとしているが、さらに多くのコンテンツ供給システムを含むとしてもよい。

【0294】また、1個のコンテンツ供給システム内において、1個の木構造を有し、前記1個の木構造を用いて、鍵を管理しているが、1個のコンテンツ供給システム内において、複数の木構造を有し、前記複数の木構造を用いて、鍵を管理するとしてもよい。このとき、複数の公開簿が公開される。また、1個のコンテンツ供給システム内において、複数のコンテンツ供給装置を含むとしてもよい。

40 【0295】また、例えば、音楽配信システム2において、音楽配信システム管理装置200と音楽コンテンツ配信装置300とは、一体の装置であるとしてもよい。また、暗号化データ配信システム1において、3個のコンテンツ供給システムが含まれ、3個のコンテンツ供給システムにおいて、それぞれ異なる公開簿の生成及び鍵管理方法を採用しているが、これらのうち、2個のコンテンツ供給システムにおいて、同一の公開簿生成方法及び同一の鍵管理方法を採用するとしてもよい。

【0296】(2) 以上述べた具体例1～具体例4で求めた各利用者機器におけるノード鍵は、使用した後、利用者機器やシステムに依存して運用、管理することができる。例えば、頻繁にそのシステムを利用する場合や、多くのメモリを備えた利用者機器であれば、そのまま保管しておけば、上記計算しなくともすぐに利用することができる。

【0297】また、あまりそのシステムを利用しない場合や、小さなメモリしかない利用者機器では、そのたびに必要なノード鍵を計算したほうが効率的である。リーフから途中の層までのノード鍵をメモリに保管し、それから上位は計算で求める等、柔軟に運用することもできる。また、もし、利用者機器が不適に搾取されてしまった場合を考慮すると、ノード鍵を機器の中に保管していないほうが良いこともある。システム管理装置は、ある利用者機器が搾取されたことが判明したら、その利用者機器がより上位層のノード鍵を求めるための情報を公開簿から消してしまう。このことにより、搾取された利用者機器をグループからはずすことができる。公開簿を先にコピーされていたら、搾取してすぐにノード鍵を求めて保管しておくなども可能なので、ある利用者機器をグループからはずす方法としては完全ではないが、簡易に対応できるため運用上は有効である。この場合には、計算したノード鍵による処理が終了したら削除するよう、システム管理装置から利用者機器に指示する。

【0298】(3) また、上記の具体例1～具体例4の各方法を組み合わせてもかまわない。例えば、木構造のリーフから1つ上の層のノード鍵を求めるためには、具体例1を用いて、それから上位の層のノード鍵を求めるためには具体例4の方法を用いるなどである。

(4) また、ここでの公開簿を利用者機器に供給する場合は、例えばシステムが管理するWebページやDVDなどのパッケージメディアを用いればよい。またWebページやパッケージメディアはシステムに1つではなく、複数に分けて管理して配布してもよい。また、当該利用者機器に関連する部分的な公開情報だけを選んで、インターネットなどを用いて送付してもよい。

【0299】(5) また、ここで述べた木構造構築方法は、次の目的のためにも利用することができる。

(a) ある時間ごとにノード鍵を変更する。  
(b) 多くの利用者機器がグループから排除され、小さな木に分割されて暗号化鍵情報の情報量が多くなったときに、残っている利用者機器で木を整える。この後、暗号化鍵情報量を初期状態に戻すことが出来る。

【0300】(6) システム管理者とコンテンツ供給者を分けており、同一機関であってもよい。つまり、システム管理装置とコンテンツ供給装置とが同一の装置であってもよい。

(7) 各利用者機器は、機器鍵から対応するシステム用機器鍵を、コンテンツ供給システムの運用開始時に都度

作成するとしているが、コンテンツ供給システムから供給されるものであっても良いし、機器作成時にシステム用機器鍵がすでに決っているコンテンツ供給システムであれば予め利用者機器に埋め込んでおいてもよい。

【0301】(8) コンテンツを任意に生成したグループ鍵で暗号化し、さらに、グループ鍵を有するノード鍵で暗号化する場合で説明したが、より一般的に単なるデータを有するノード鍵で暗号化するとしてもよい。

(9) コンテンツ供給システムを例にして、コンテンツ供給システムごとにシステム管理者とコンテンツ配信者が存在する場合で説明したが、より一般的に単なる暗号化装置としてもよい。

【0302】(10) 上記に説明した複数の木構造は、それぞれ、4階層から構成される2分木であるとしているが、これには限定されない。前記複数の木構造は、さらに多くの階層を有しているとしてもよいし、また、前記複数の木構造は、それぞれ異なる階層数の木構造からなるとしてもよい。また、前記複数の木構造は、3分木、4分木などであるとしてもよい。前記複数の木構造は、一般的に、n分木であるとしてもよい。ここで、nは、2以上の整数である。

【0303】(11) 上記に説明した各コンテンツ供給システムは、音楽及び映画のコンテンツを供給するとしているが、他のコンテンツを供給するとしてもよい。また、上記に説明した各コンテンツ供給システムは、インターネット、DVDなどのパッケージメディア、放送メディアを介して、コンテンツを供給するとしているが、他のメディアを介して、コンテンツを供給するとしてもよい。

【0304】(12) 上記に説明した鍵管理装置は、利用者機器に固有の機器鍵を生成するとしているが、これには限定されない。例えば、利用者機器が自身で固有の機器鍵を生成し、生成した機器鍵を鍵管理装置に秘密に登録するようにしてもよい。

(13) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0305】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0306】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は

有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0307】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。  
 10 (1) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### 【0308】

【発明の効果】今後、1個の利用者機器が、複数のコンテンツ供給システムに接続されることが予測できる。例えば、STB(セットトップボックス)は、家庭内の機器のゲートウェイマシンの役割を担い、パッケージメディア、放送、インターネットなどに接続されると予測される。このため、STBは、複数のコンテンツ供給システムに対応する必要がある。一方で、前記複数のコンテンツ供給システムにおいて、それぞれ用いられる暗号化のための鍵の管理方法が1つに統一されることは困難であると思われる。

【0309】ある利用者機器が、複数システムの木構造鍵管理に対応するために、次の2つの方法が考えられる。

(第1の方法) 共通の1つの木構造を利用する。

(第2の方法) 1個の利用者機器が、コンテンツ供給システムにおいて個別に定められたそれぞれ独立した木構造を備える。つまり、利用者機器は、複数の木構造のリーフからルートに至るノード鍵をすべて保持する。

#### 【0310】上記2つの方法には、以下の課題がある。

(a) 柔軟性の欠如(第1及び第2の方法に共通の課題)

第2の方法では、利用者機器の製造時に、利用者機器で使用するコンテンツ供給システムをすべて決め、あらかじめ対応するノード鍵を格納しておく必要がある。このため、利用者機器を製造して利用者に提供した後に、利用者機器を新たなコンテンツ供給システムに追加させるためには、例えば、ICカードのような安全なデバイスを用いて利用者機器にノード鍵を追加するなど、特別な仕組みが必要となる。

【0311】また、第1の方法では、例えば、コンテンツ供給システムが任意の加入機器集合を1つにまとめて鍵を配布したい場合も、木構造が定まっているため、ばらばらに配布する必要があり、暗号化鍵情報が増加し非効率である。

(b) システム間の密匿性の欠如(第1の方法の課題)  
 第1の方法では、コンテンツ供給システムのシステム管理者は、木のすべてのノード鍵を共有している。あるコンテンツ供給システムで用いるグループ鍵は、別のコンテンツ供給システムのシステム管理者に知られ得る。

【0312】(c) 機器の秘密に保持する鍵の容量が多い(第2の方法の課題)

第2の方法では、利用者機器はリーフからルートに至るノード鍵を、それぞれのコンテンツ供給システムの木構造に対応してすべて秘密に保存する必要がある。利用者機器が加入するコンテンツ供給システムが多ければ、利用者機器内の秘密の鍵保存用に大きなメモリが必要となる。

【0313】ところが、以上説明したように、本発明によれば、1個の利用者機器が複数のコンテンツ供給システムに接続される場合に、それぞれのコンテンツ供給システムが柔軟で独自の木構造を用いたグループ鍵管理方法を使用することが可能になる。具体的には、鍵管理装置は、コンテンツ供給システムのシステム管理装置に対して、一方向性関数を施したシステム用機器鍵だけを配布する。システム管理装置は、システム用機器鍵を用いて、鍵を管理し、公開簿を生成する。各利用者機器は木構造のリーフに対応する機器鍵だけを保持し、機器鍵と各コンテンツ供給システム用の公開簿を用いて、木構造の下から上に順次対応するノード鍵を求める。

【0314】また、本発明によると、不正に暴露された特定の端末だけを排除し、その他の端末ではコンテンツの再生等が可能でありながら、記録メディアに格納される暗号化されたデータを少なく抑えることができる。また、本発明によると、次の特徴を有する。

(a) コンテンツ供給システムごとに自由に木構造を構築することができる。また、コンテンツ供給システムの追加も可能である。

(b) コンテンツ供給システムで用いる木構造に用いられるノード鍵とグループ鍵を、別のコンテンツ供給システムのシステム管理者が知ることは困難である。

(c) 機器は1つの固有機器鍵のみを保管すればよい。

【0315】以上説明したように、本発明は、鍵管理装置と複数のコンテンツ供給装置と1個以上の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、各利用者機器は、暗号化コンテンツを復号して利用し、各利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、それぞれ、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジ

タル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機器へ出力する複数のコンテンツ供給装置と、それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成し、生成した前記第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する1個以上の利用者機器とから構成される。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおいて、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を供給し、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、前記利用者機器へ当該利用者機器に固有の機器鍵を出力する機器鍵出力手段と、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した第1システム用機器鍵を前記コンテンツ供給装置へ出力するシステム用機器鍵生成手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している記憶手段と、前記鍵管理装置から前記第1システム用機器鍵を取得する取得手段と、前記第1システム用機器鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、受け取った前記第1システム用機器鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを利用者機

器へ出し、前記鍵管理装置から前記機器鍵を受け取る取得手段と、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る受信手段と、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成手段と、生成した第2システム用機器鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

【0316】これらの構成によると、各コンテンツ供給装置は、柔軟で独自の鍵の管理を行うことができる。ここで、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムであって、各コンテンツ供給装置は、それぞれ暗号化コンテンツを供給し、前記利用者機器は、暗号化コンテンツを復号して利用し、前記利用者機器へ当該利用者機器に固有の機器鍵を出し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、それぞれ、前記第1システム用機器鍵を受け取り、前記第1システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出し、前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開する複数のコンテンツ供給装置と、それぞれ、前記機器鍵を受け取り、前記暗号化コンテンツを受け取り、公開された前記公開簿を取得し、前記機器鍵及び前記コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成し、前記第2システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する1個の利用者機器とから構成される。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している記憶手段と、前記鍵管理装置から前記第1システム用機器鍵を取得する取得手段と、前記第1

システム用機器鍵を当該コンテンツ供給装置へ出力する鍵管理装置と、それぞれ、前記第1システム用機器鍵を受け取り、前記暗号化コンテンツを受け取り、前記デバイス鍵を決定し、決定した前記デバイス鍵に基づいて、前記デバイス鍵を特定し、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する1個の利用者機器とから構成される。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記コンテンツ供給装置であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出力し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出力し、デジタル著作物であるコンテンツを記憶している記憶手段と、前記鍵管理装置から前記第1システム用機器鍵を取得する取得手段と、前記第1

システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、前記コンテンツを暗号化して暗号化コンテンツを生成する暗号手段と、前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成する公開簿生成手段と、生成した前記公開簿を公開し、生成した前記暗号化コンテンツを利用者機器へ出力する出力手段とを備える。また、鍵管理装置と複数のコンテンツ供給装置と1個の利用者機器とから構成されるデータ配信システムにおける前記利用者機器であって、前記鍵管理装置は、前記利用者機器へ当該利用者機器に固有の機器鍵を出し、各コンテンツ供給装置について、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて一方向性関数を用いて前記利用者機器に固有の第1システム用機器鍵を生成し、生成した前記第1システム用機器鍵を当該コンテンツ供給装置へ出し、各コンテンツ供給装置は、前記第1システム用機器鍵を受け取り、前記第1システム用機器鍵に基づいて、コンテンツを暗号化する際に基づくデバイス鍵を決定し、決定した前記デバイス鍵に基づいて、デジタル著作物であるコンテンツを暗号化して暗号化コンテンツを生成し、前記暗号化コンテンツを前記利用者機器へ出力し、前記第1システム用機器鍵に基づいて、前記デバイス鍵を特定するための公開簿を生成し、生成した前記公開簿を公開し、前記鍵管理装置から前記機器鍵を受け取り、公開された前記公開簿を取得し、前記コンテンツ供給装置から前記暗号化コンテンツを受け取る取得手段と、前記機器鍵及び当該コンテンツ供給装置に固有のシステム情報に基づいて前記一方向性関数を用いて前記利用者機器に固有の第2システム用機器鍵を生成するシステム用機器鍵生成手段と、前記第2システム用機器鍵に基づいて、前記公開簿から前記デバイス鍵を特定するデバイス鍵特定手段と、特定した前記デバイス鍵に基づいて、受け取った前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

【0317】これらの構成によると、利用者機器に割り当てられるデバイス鍵に基づいて、コンテンツが暗号化され、利用者機器は、公開される公開簿からデバイス鍵を取得でき、取得したデバイス鍵により暗号化コンテンツを復号できるので、当該利用者機器以外の機器により、暗号化コンテンツが不用意に復号されることがない。

【0318】また、前記コンテンツ供給装置は、前記第1システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、前記利用者機器は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定する。また、前記コンテンツ供給装置は、前記第1システム用機

器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定し、前記デバイス鍵を用いて前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造を用いて、前記公開簿から、前記デバイス鍵を特定する。また、前記暗号手段は、前記第1システム用機器鍵がリーフに割り当てられ、他のノードにノード鍵が割り当てられた木構造を備え、前記木構造を用いて管理されている1個以上のノード鍵の中から前記デバイス鍵を決定する。

【0319】これらの構成によると、木構造を用いて鍵を管理するので、コンテンツ供給装置が管理すべき鍵情報のデータ量を少なくすることができる。前記コンテンツ供給装置は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、公開し、前記利用者機器は、Webサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得する。また、前記出力手段は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、公開する。また、前記コンテンツ供給装置は、生成した前記公開簿を、Webサーバ、パッケージメディア又は放送メディアを介して、前記取得手段は、Webサーバ、パッケージメディア又は放送メディアを介して、前記公開簿を取得する。

【0320】これらの構成によると、公開される暗号化鍵情報は、Webサーバ、パッケージメディア、又は放送メディアを介して利用者機器へ送信されるので、利用者機器は、いずれかのメディアを介して、容易に暗号化鍵情報を取得することができる。ここで、前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する情報のみを出し、前記利用者機器は、前記公開簿のうち、前記利用者機器に関連する情報のみを取得する。また、前記公開簿生成手段は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成し、前記出力手段は、前記利用者機器関連情報を、公開する。また、前記コンテンツ供給装置は、前記公開簿のうち、前記利用者機器に関連する利用者機器関連情報のみを生成して公開し、前記取得手段は、前記利用者機器関連情報を取得し、前記デバイス鍵特定手段は、取得した前記利用者機器関連情報から当該利用者機器に対応する前記デバイス鍵を特定する。

【0321】これらの構成によると、暗号化鍵情報のうち、利用者機器に関連する情報のみが利用者機器に送信されるので、送信されるデータ量を少なく抑えることができる。ここで、前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成する。また、前記コンテンツ供給装置は、前記木構造のリ

ーフを除く各ノードについて、当該ノードに割り当てられたノード鍵を、当該ノードの子ノードに割り当てられたノード鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を含む前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を用いて、取得した前記公開簿内の暗号化ノード鍵を復号して、当該ノードの親ノードのノード鍵を求める。

【0322】これらの構成によると、子ノード鍵で親ノード鍵を暗号化し、暗号化親ノード鍵を復号して子ノード鍵を求めることができるので、木構造の子ノードから親ノードの方向へ向かって、ノード鍵を求めることができる。ここで、前記公開簿生成手段は、前記木構造のリーフを除く各ノードについて、(a) 当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、(b) 当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、(c) 生成した暗号化ノード鍵を含む前記公開簿を生成する。また、前記コンテンツ供給装置は、前記木構造のリーフを除く各ノードについて、

(a) 当該ノードの1個の子ノードに割り当てられたノード鍵に一方向性関数を施して、当該ノードのノード鍵を生成し、(b) 当該ノードの別の子ノードに割り当てられたノード鍵を用いて、生成した当該ノードのノード鍵を暗号化して暗号化ノード鍵を生成し、(c) 生成した暗号化ノード鍵を含む前記公開簿を生成し、前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を用いて公開された公開簿内の暗号化ノード鍵を復号した復号文、又は当該ノードに対応するノード鍵に一方向性関数を施して得られた出力値を選択し、選択した値を当該ノードの親ノードのノード鍵として求める。

【0323】これらの構成によると、親ノード鍵の生成の一部において、子ノード鍵に一方向性関数を施して親ノード鍵を生成するので、公開される暗号化鍵情報のデータ量を少なく抑えることができる。ここで、 $k$ を2以上の整数とし、 $m$ を0以上の整数とし、前記木構造を $k$ 分木とし、各ノード鍵を $(x, y)$ 平面上の点とみなし、前記公開簿生成手段は、 $(x, y)$ 平面上において、共通の親ノードを持つ $k$ 個の全てのノードのノード鍵を結ぶ $(k+m-1)$ 次の曲線を生成し、前記曲線上のノード鍵以外の $(k+m-1)$ 個の点を含む前記公開簿を生成する。また、 $k$ を2以上の整数とし、 $m$ を0以上の整数とし、前記木構造を $k$ 分木とし、各ノード鍵を $(x, y)$ 平面上の点とみなし、前記コンテンツ供給装置は、 $(x, y)$ 平面上において、共通の親ノードを持つ $k$ 個の全てのノードのノード鍵を結ぶ $(k+m-1)$ 次の曲線を生成し、前記曲線上のノード鍵以外の $(k+m-1)$ 個の点を含む前記公開簿を生成し、前記デバイ

10 10 20 30 40 50

ス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵と、公開された公開簿内の $(k+m-1)$ 個の点とを結ぶ、 $(k+m-1)$ 次の曲線を求め、さらにこの曲線から一方向性関数を用いて当該ノードの親ノードに対応するノード鍵を求める。

【0324】これらの構成によると、安全性を保つつつ、確実にノード鍵を復号できる。ここで、前記公開簿生成手段は、(a) 公開鍵暗号の秘密鍵と公開鍵のペアを生成し、(b) 生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、(c) 前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、前記出力手段は、前記公開簿を公開する。また、前記コンテンツ供給装置は、(a) 公開鍵暗号の秘密鍵と公開鍵のペアを生成し、(b) 生成した前記秘密鍵を秘密に保持し、生成した前記公開鍵を含む前記公開簿を生成し、(c) 前記木構造のリーフを除くノードについて、当該ノードに対応するノード鍵に基づいて、前記秘密鍵を用いて暗号化して暗号化ノード鍵を生成し、生成した暗号化ノード鍵を、当該ノードの子ノードに対応するノード鍵とし、(d) 前記公開簿を公開し、前記デバイス鍵特定手段は、前記木構造の1個のノードに対応するノード鍵を、公開された公開簿内の公開鍵を用いて復号し、その結果を当該ノードの親ノードに対応するノード鍵とする。

【0325】これらの構成によると、公開鍵暗号方式を用いるので、安全性を保つつつ、確実にノード鍵を復号できる。

【図面の簡単な説明】

【図1】暗号化データ配信システム1の構成を示すブロック図である。

【図2】鍵管理装置100の構成を示すブロック図である。

【図3】機器鍵管理テーブル111のデータ構造を示す。

【図4】システム用機器鍵管理テーブル121のデータ構造を示す。

【図5】音楽配信システム管理装置200の構成を示すブロック図である。

【図6】木構造T100を示す概念図である。

【図7】音楽配信用木構造テーブル211のデータ構造を示す。

【図8】音楽用公開簿221のデータ構造を示す。

【図9】公開簿サーバ装置400の構成を示すブロック図である。

【図10】音楽コンテンツ配信装置300の構成を示すブロック図である。

【図11】DVD供給システム管理装置500の構成を

示すブロック図である。

【図12】DVD用木構造テーブル511のデータ構造を示す。

【図13】木構造T200を示す概念図である。

【図14】DVD用公開簿521のデータ構造を示す。

【図15】映画放送システム管理装置800の構造を示すブロック図である。

【図16】木構造T300を示す概念図である。

【図17】映画放送用木構造テーブル811のデータ構造を示す。

【図18】公開簿生成部806による公開簿生成の手順を示すx-y座標空間上の概念図である。

【図19】木構造T300の一部分を示す概念図である。

【図20】映画用公開簿821のデータ構造を示す。

【図21】利用者機器1100の構造を示すブロック図である。

【図22】鍵管理装置100の動作を示すフローチャートである。

【図23】音楽配信システム管理装置200の動作を示すフローチャートである。

【図24】公開簿生成部206による音楽用公開簿の生成の動作を示すフローチャートである。図25へ続く。

【図25】公開簿生成部206による音楽用公開簿の生成の動作を示すフローチャートである。図24から続く。

【図26】音楽コンテンツ配信装置300の動作を示すフローチャートである。

【図27】DVD供給システム管理装置500の全体の動作を示すフローチャートである。

【図28】ノード鍵生成部505によるノード鍵の生成の動作を示すフローチャートである。

【図29】公開簿生成部506によるDVD用公開簿の生成の動作を示すフローチャートである。図30へ続く。

【図30】公開簿生成部506によるDVD用公開簿の生成の動作を示すフローチャートである。図29から続く。

【図31】映画放送システム管理装置800の動作を示すフローチャートである。図32へ続く。

【図32】映画放送システム管理装置800の動作を示すフローチャートである。図33へ続く。

【図33】映画放送システム管理装置800の動作を示すフローチャートである。図32から続く。

【図34】利用者機器1100全体の動作を示すフローチャートである。

【図35】ノード鍵特定部1103によるノード鍵の特定(1)の動作を示すフローチャートである。図36へ続く。

【図36】ノード鍵特定部1103によるノード鍵の特

定(1)の動作を示すフローチャートである。図35から続く。

【図37】ノード鍵特定部1103によるノード鍵の特定(2)の動作を示すフローチャートである。図38へ続く。

【図38】ノード鍵特定部1103によるノード鍵の特定(2)の動作を示すフローチャートである。図39へ続く。

【図39】ノード鍵特定部1103によるノード鍵の特定(2)の動作を示すフローチャートである。図40へ続く。

【図40】ノード鍵特定部1103によるノード鍵の特定(2)の動作を示すフローチャートである。図39から続く。

【図41】ノード鍵特定部1103によるノード鍵の特定(3)の動作を示すフローチャートである。図42へ続く。

【図42】ノード鍵特定部1103によるノード鍵の特定(3)の動作を示すフローチャートである。図43へ続く。

【図43】ノード鍵特定部1103によるノード鍵の特定(3)の動作を示すフローチャートである。図42から続く。

【図44】木構造T400を示す概念図である。

【図45】音楽配信用木構造テーブル211bのデータ構造を示す。

【図46】音楽用公開簿221bのデータ構造を示す。

【図47】音楽配信システム管理装置200bの動作を示すフローチャートである。図48へ続く。

【図48】音楽配信システム管理装置200bの動作を示すフローチャートである。図49へ続く。

【図49】音楽配信システム管理装置200bの動作を示すフローチャートである。図50へ続く。

【図50】音楽配信システム管理装置200bの動作を示すフローチャートである。図51へ続く。

【図51】音楽配信システム管理装置200bの動作を示すフローチャートである。図50から続く。

【図52】利用者機器1100bの動作のうち、ノード鍵特定部1103bによるノード鍵の特定(1)の動作を示すフローチャートである。図53へ続く。

【図53】利用者機器1100bの動作のうち、ノード鍵特定部1103bによるノード鍵の特定(1)の動作を示すフローチャートである。図52から続く。

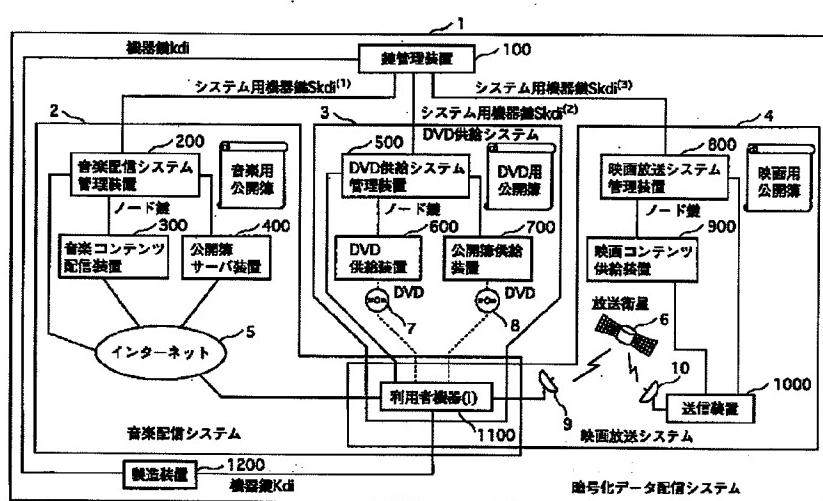
【図54】非特許文献1により開示されている木構造分割方法における木構造を示す概念図である。

#### 【符号の説明】

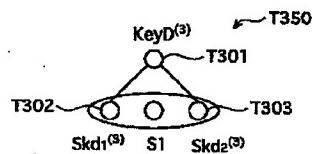
- 1 暗号化データ配信システム
- 2 音楽配信システム
- 3 DVD供給システム
- 4 映画放送システム

100	鍵管理装置	*	700	公開簿供給装置
200	音楽配信システム管理装置		800	映画放送システム管理装置
300	音楽コンテンツ配信装置		900	映画コンテンツ供給装置
400	公開簿サーバ装置		1000	送信装置
500	DVD供給システム管理装置		1100	利用者機器
600	DVD供給装置	*	1200	製造装置

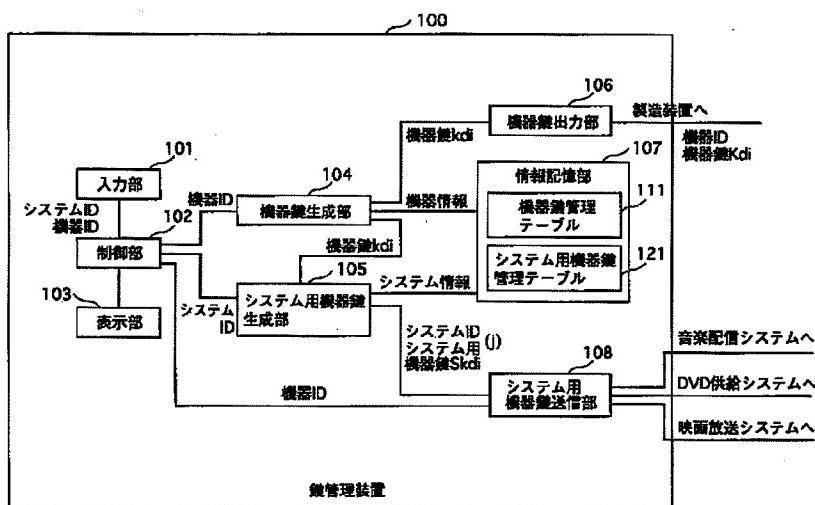
【図1】



【図19】



【図2】



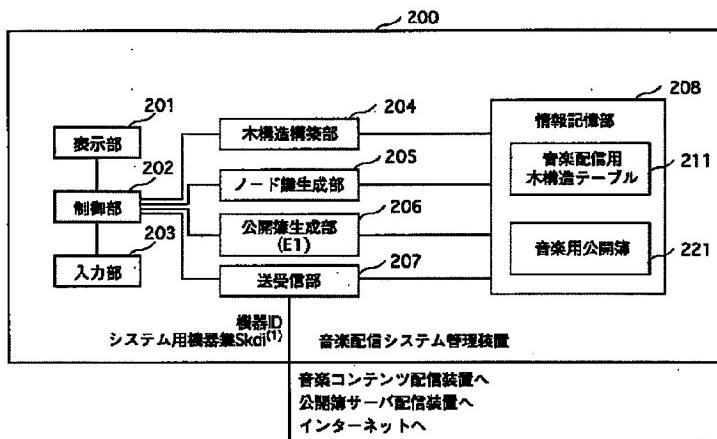
【図3】

機器管理テーブル	
機器ID	機器鍵Skdi
1001	kd1
1002	kd2
1003	kd3
⋮	⋮

【図4】

システム用機器管理テーブル		
機器ID	システムID (1)	システム用機器鍵Skdi <sup>(1)</sup>
1001	1	Skd1 <sup>(1)</sup>
1002	1	Skd2 <sup>(1)</sup>
1003	1	Skd3 <sup>(1)</sup>
⋮	⋮	⋮
1001	2	Skd1 <sup>(2)</sup>
1002	2	Skd2 <sup>(2)</sup>
1003	2	Skd3 <sup>(2)</sup>
⋮	⋮	⋮

【図5】



【図7】

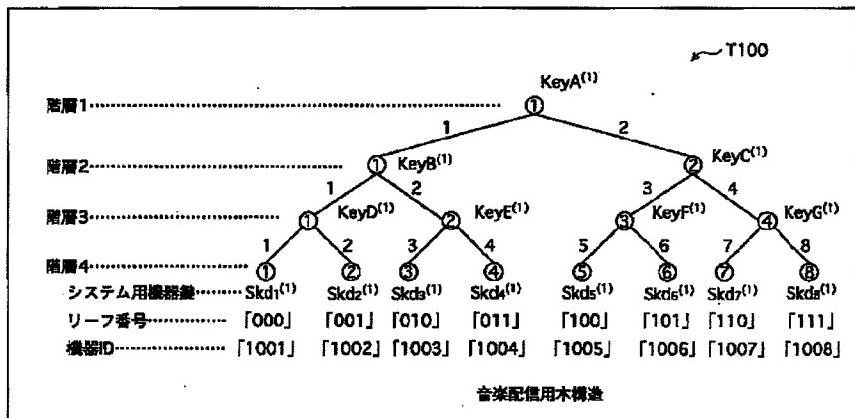
音楽配信用木構造テーブル			
階層番号	ノード番号	ノード鍵	機器ID
1	1	KeyA <sup>(1)</sup>	—
2	1	KeyB <sup>(1)</sup>	—
2	2	KeyC <sup>(1)</sup>	—
3	1	KeyD <sup>(1)</sup>	—
3	2	KeyE <sup>(1)</sup>	—
3	3	KeyF <sup>(1)</sup>	—
3	4	KeyG <sup>(1)</sup>	—
4	1	Skd1 <sup>(1)</sup>	1001
4	2	Skd2 <sup>(1)</sup>	1002
4	3	Skd3 <sup>(1)</sup>	1003
4	4	Skd4 <sup>(1)</sup>	1004
4	5	Skd5 <sup>(1)</sup>	1005
4	6	Skd6 <sup>(1)</sup>	1006
4	7	Skd7 <sup>(1)</sup>	1007
4	8	Skd8 <sup>(1)</sup>	1008

【図14】

DVD用公開鍵

システムID	2
公開情報	
インデックス情報 (階層番号、ノード番号)	暗号化ノード鍵
(3, 1)	E4(Skd3 <sup>(2)</sup> , KeyD <sup>(2)</sup> )
(3, 2)	E4(Skd4 <sup>(2)</sup> , KeyE <sup>(2)</sup> )
(3, 3)	E4(Skd5 <sup>(2)</sup> , KeyF <sup>(2)</sup> )
(3, 4)	E4(Skd6 <sup>(2)</sup> , KeyG <sup>(2)</sup> )
(2, 1)	E4(KeyE <sup>(2)</sup> , KeyB <sup>(2)</sup> )
(2, 2)	E4(KeyG <sup>(2)</sup> , KeyC <sup>(2)</sup> )
(1, 1)	E4(KeyC <sup>(2)</sup> , KeyA <sup>(2)</sup> )

【図6】



【図8】

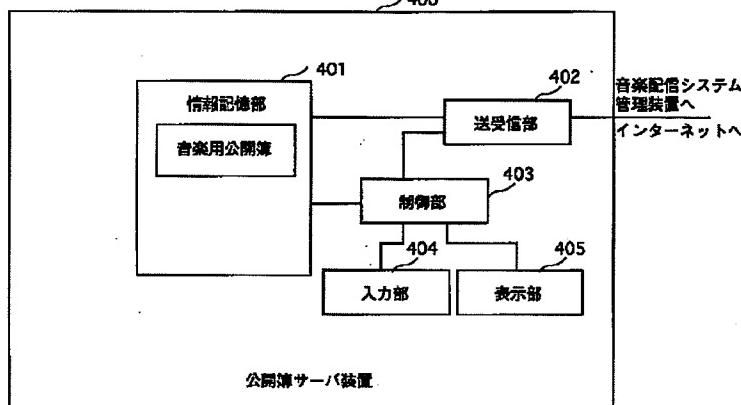
音楽用公開簿

221

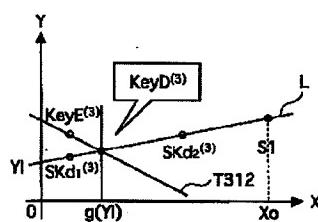
システムID	1
公開情報	
インデックス情報 (階層番号、パス番号)	暗号化ノード鍵
(3, 1)	E1(Skd1 <sup>(1)</sup> ,KeyD <sup>(1)</sup> )
(3, 2)	E1(Skd2 <sup>(1)</sup> ,KeyD <sup>(1)</sup> )
(3, 3)	E1(Skd3 <sup>(1)</sup> ,KeyE <sup>(1)</sup> )
(3, 4)	E1(Skd4 <sup>(1)</sup> ,KeyE <sup>(1)</sup> )
(3, 5)	E1(Skd5 <sup>(1)</sup> ,KeyF <sup>(1)</sup> )
(3, 6)	E1(Skd6 <sup>(1)</sup> ,KeyF <sup>(1)</sup> )
(3, 7)	E1(Skd7 <sup>(1)</sup> ,KeyG <sup>(1)</sup> )
(3, 8)	E1(Skd8 <sup>(1)</sup> ,KeyG <sup>(1)</sup> )
(2, 1)	E1(KeyD <sup>(1)</sup> ,KeyB <sup>(1)</sup> )
(2, 2)	E1(KeyE <sup>(1)</sup> ,KeyB <sup>(1)</sup> )
(2, 3)	E1(KeyF <sup>(1)</sup> ,KeyC <sup>(1)</sup> )
(2, 4)	E1(KeyG <sup>(1)</sup> ,KeyC <sup>(1)</sup> )
(1, 1)	E1(KeyB <sup>(1)</sup> ,KeyA <sup>(1)</sup> )
(1, 2)	E1(KeyC <sup>(1)</sup> ,KeyA <sup>(1)</sup> )

【図9】

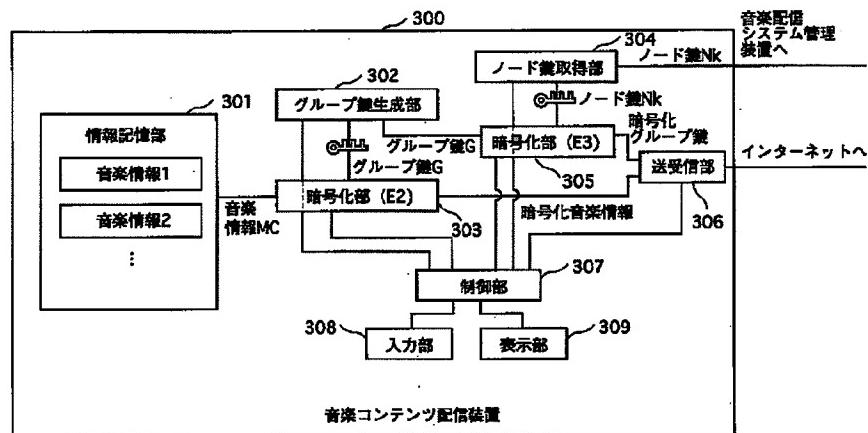
400



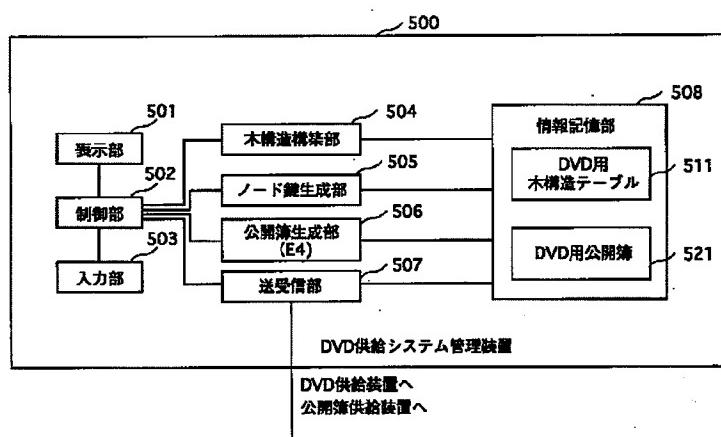
【図18】



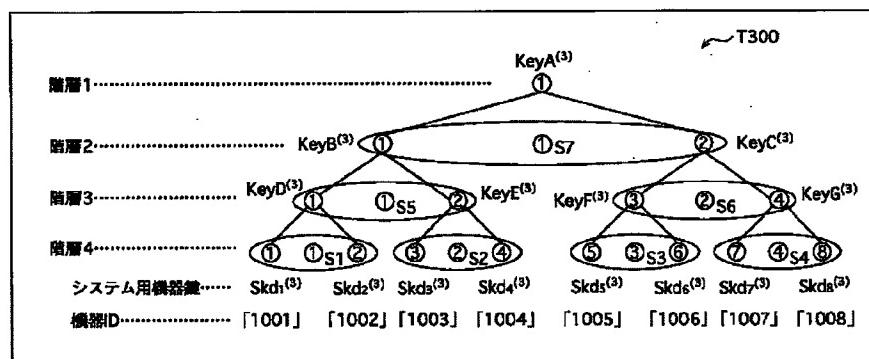
【図10】



【図11】



【図16】



【図12】

DVD用木構造テーブル

511

ノード情報			
階層番号	ノード番号	ノード鍵	機器ID
1	1	KeyA <sup>(2)</sup> =g(KeyB <sup>(2)</sup> )	-
2	1	KeyB <sup>(2)</sup> =g(KeyD <sup>(2)</sup> )	-
2	2	KeyC <sup>(2)</sup> =g(KeyF <sup>(2)</sup> )	-
3	1	KeyD <sup>(2)</sup> =g(Skd1 <sup>(2)</sup> )	-
3	2	KeyE <sup>(2)</sup> =g(Skd3 <sup>(2)</sup> )	-
3	3	KeyF <sup>(2)</sup> =g(Skd5 <sup>(2)</sup> )	-
3	4	KeyG <sup>(2)</sup> =g(Skd7 <sup>(2)</sup> )	-
4	1	Skd1 <sup>(2)</sup>	1001
4	2	Skd2 <sup>(2)</sup>	1002
4	3	Skd3 <sup>(2)</sup>	1003
4	4	Skd4 <sup>(2)</sup>	1004
4	5	Skd5 <sup>(2)</sup>	1005
4	6	Skd6 <sup>(2)</sup>	1006
4	7	Skd7 <sup>(2)</sup>	1007
4	8	Skd8 <sup>(2)</sup>	1008

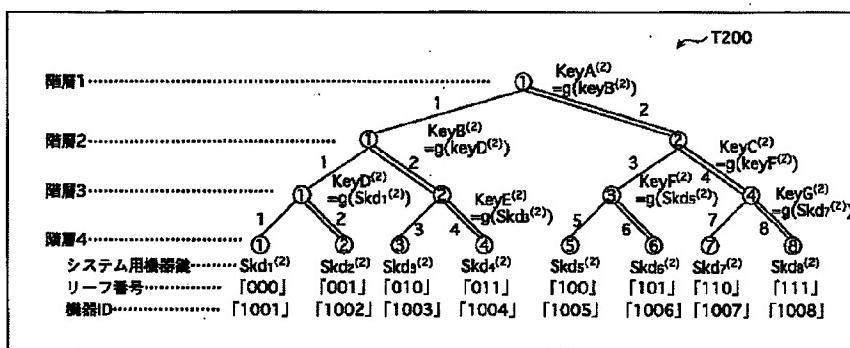
【図17】

映画放送用木構造テーブル

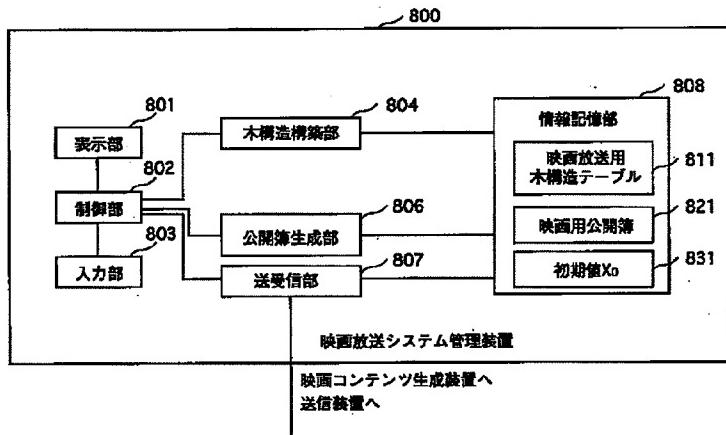
811

ノード情報			
階層番号	ノード番号	ノード鍵	機器ID
1	1	KeyA <sup>(3)</sup>	-
2	1	KeyB <sup>(3)</sup>	-
2	2	KeyC <sup>(3)</sup>	-
3	1	KeyD <sup>(3)</sup>	-
3	2	KeyE <sup>(3)</sup>	-
3	3	KeyF <sup>(3)</sup>	-
3	4	KeyG <sup>(3)</sup>	-
4	1	Skd1 <sup>(3)</sup>	1001
4	2	Skd2 <sup>(3)</sup>	1002
4	3	Skd3 <sup>(3)</sup>	1003
4	4	Skd4 <sup>(3)</sup>	1004
4	5	Skd5 <sup>(3)</sup>	1005
4	6	Skd6 <sup>(3)</sup>	1006
4	7	Skd7 <sup>(3)</sup>	1007
4	8	Skd8 <sup>(3)</sup>	1008

【図13】



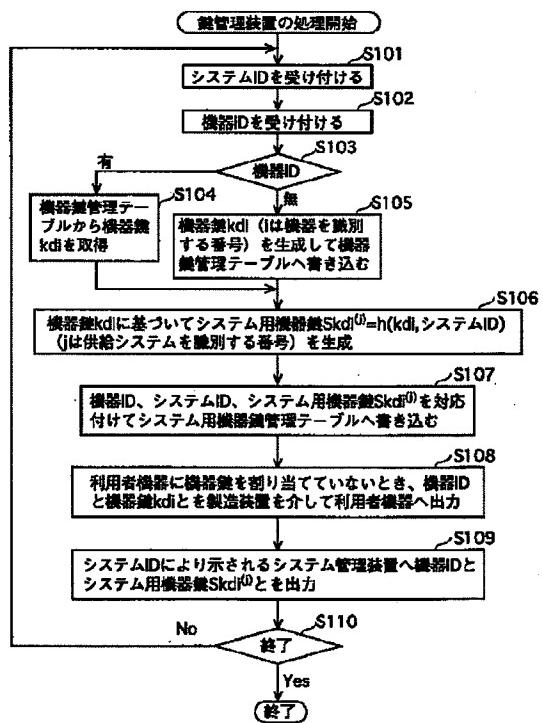
【図15】



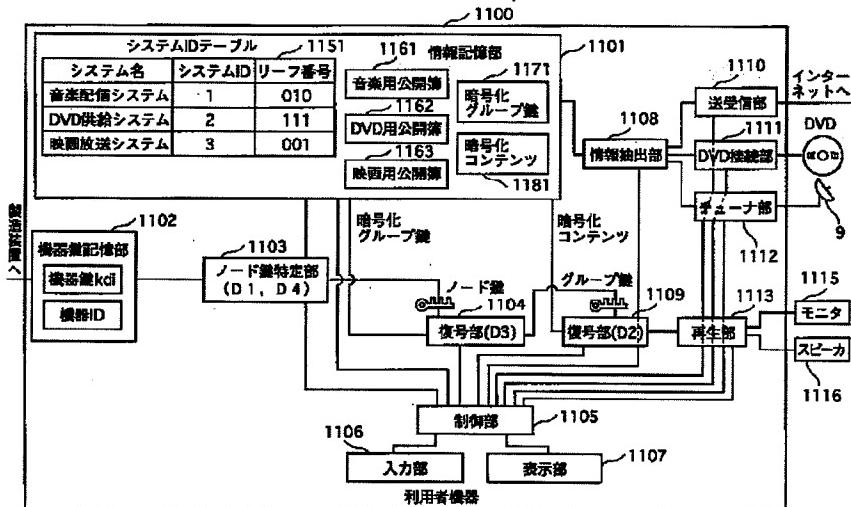
【図20】

映画用公開簿	
システムID	3
公開情報	
初期値	X <sub>0</sub>
インデックス情報 (階層番号、公開点のノード番号)	公開点y座標
(4, 1)	S <sub>1(y)</sub>
(4, 2)	S <sub>2(y)</sub>
(4, 3)	S <sub>3(y)</sub>
(4, 4)	S <sub>4(y)</sub>
(3, 1)	S <sub>5(y)</sub>
(3, 2)	S <sub>6(y)</sub>
(2, 1)	S <sub>7(y)</sub>

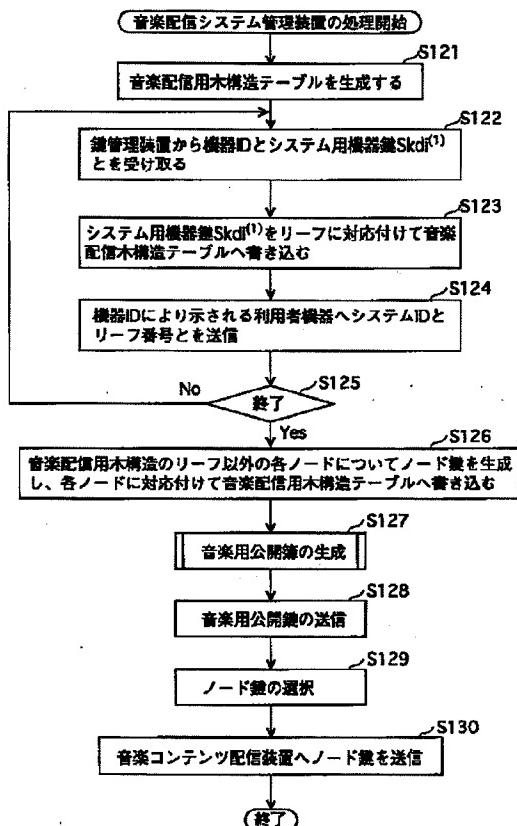
【図22】



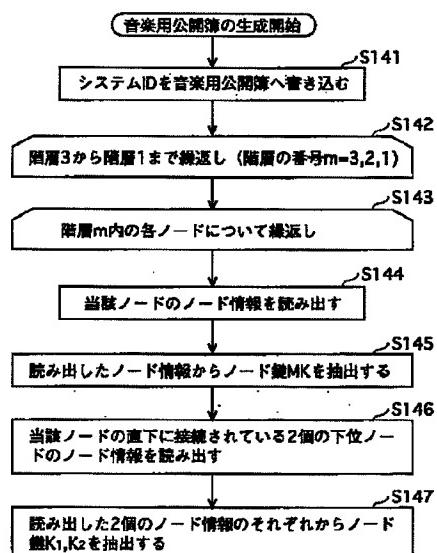
【図21】



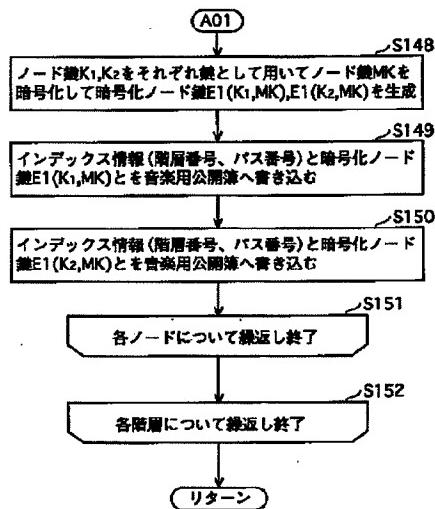
【図23】



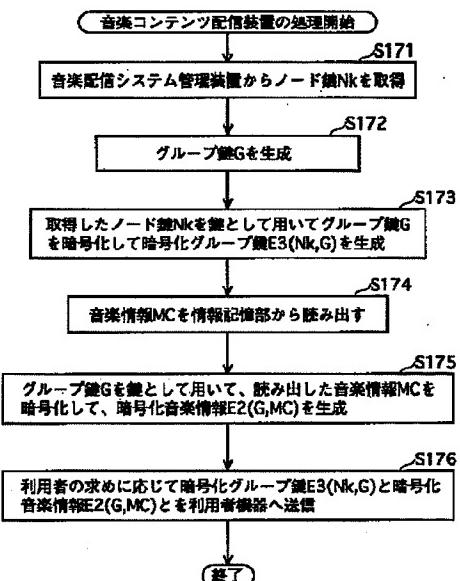
【図24】



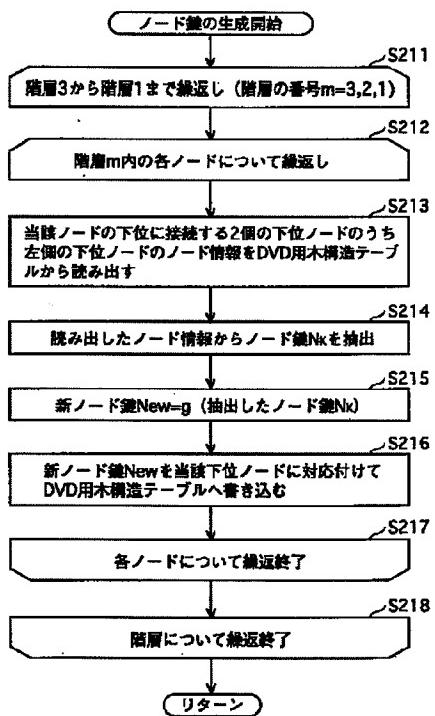
【図25】



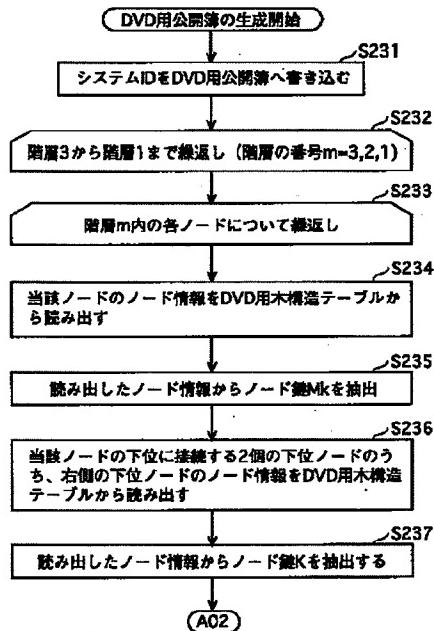
【図26】



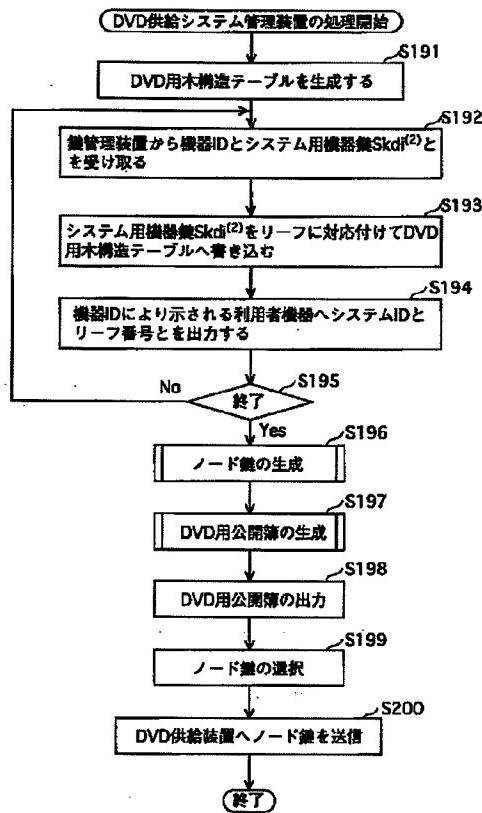
【図28】



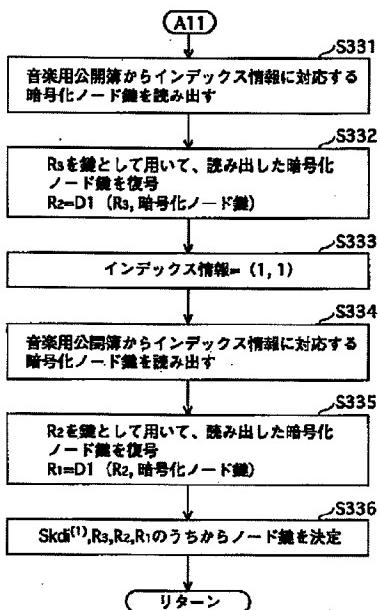
【図29】



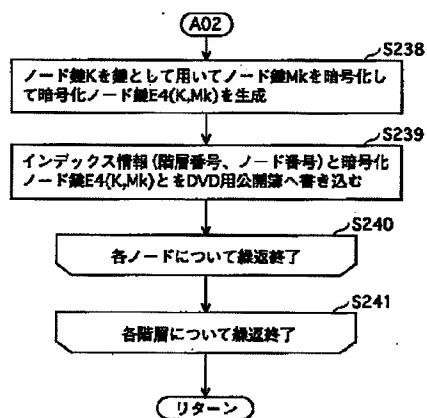
【図27】



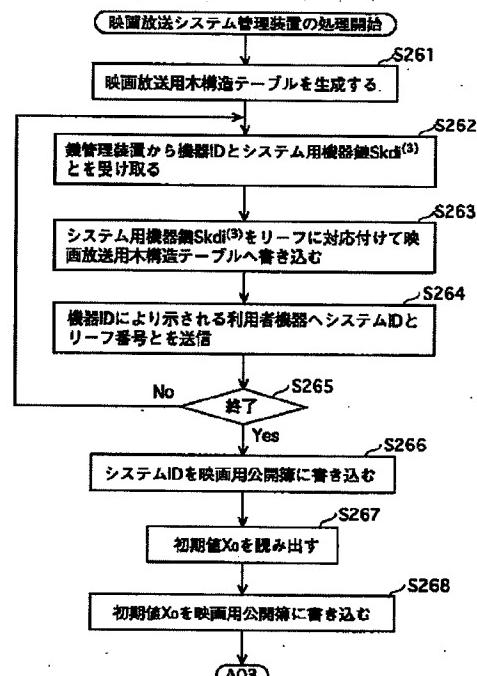
【図36】



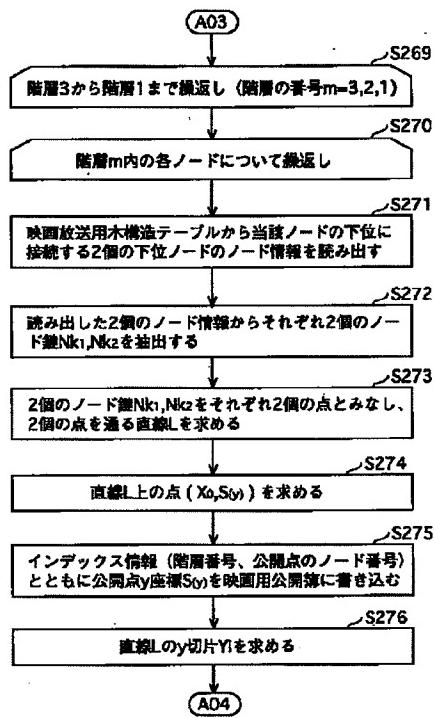
【図30】



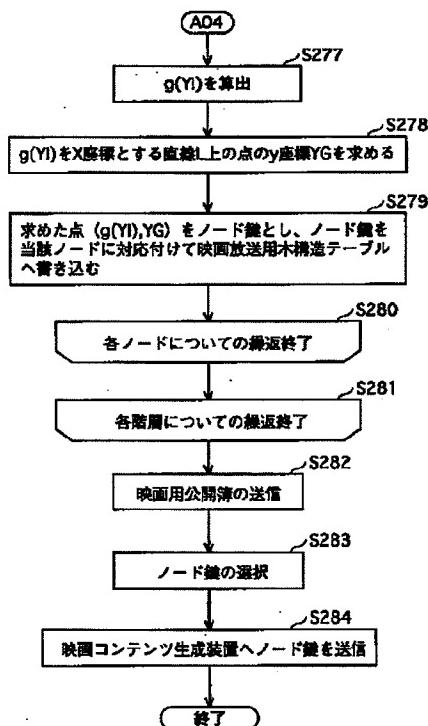
【図31】



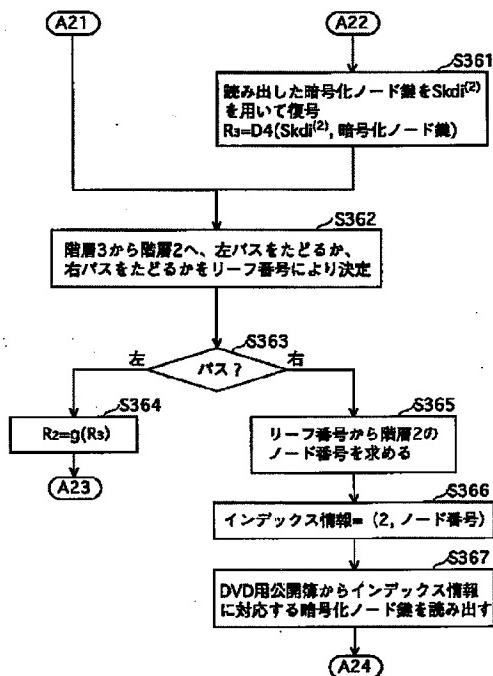
【図32】



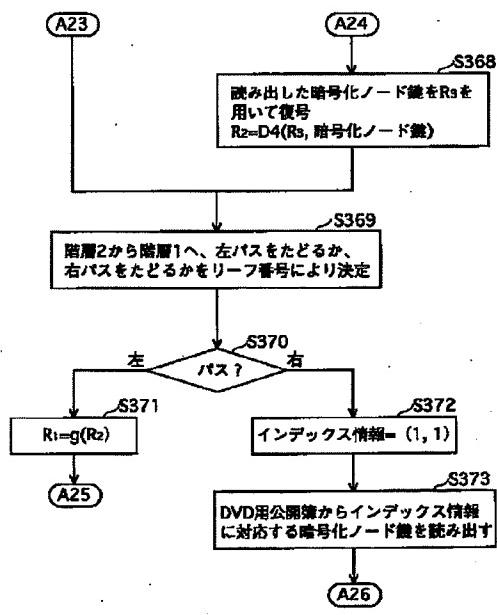
【図33】



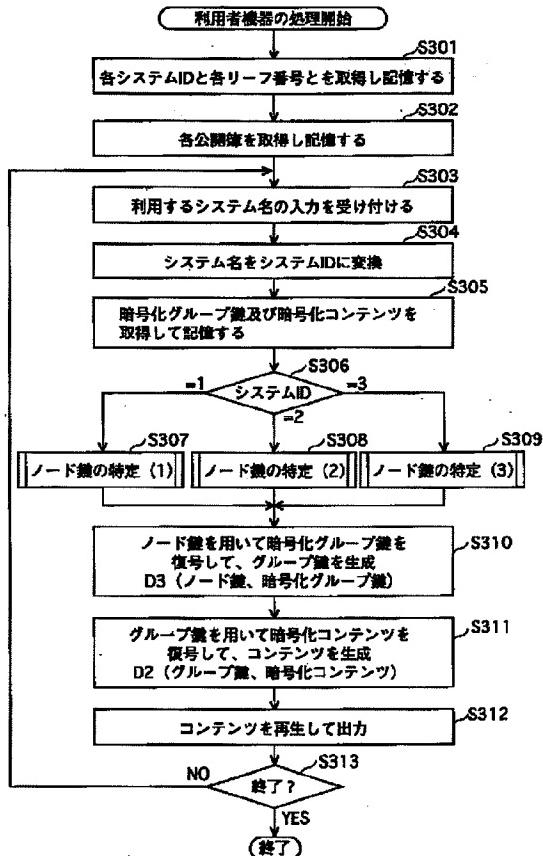
【図38】



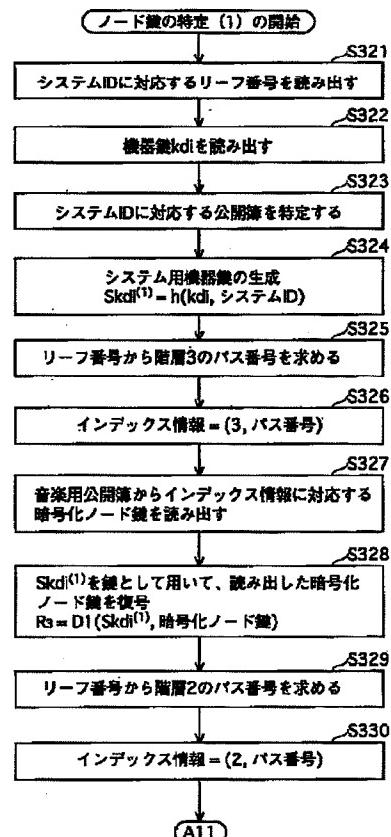
【図39】



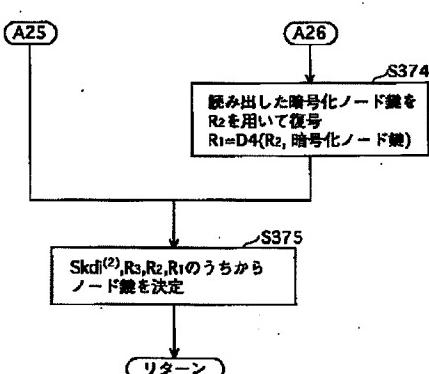
【図34】



【図35】



【図40】



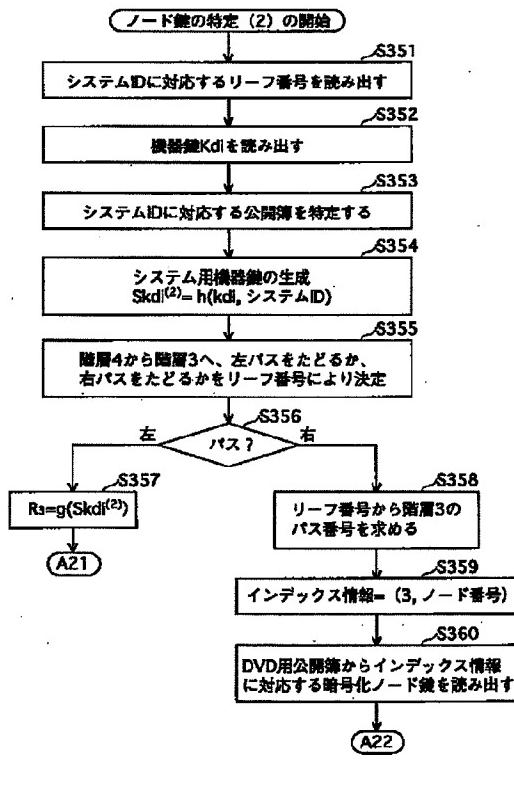
【図45】

音楽配信用木構造テーブル

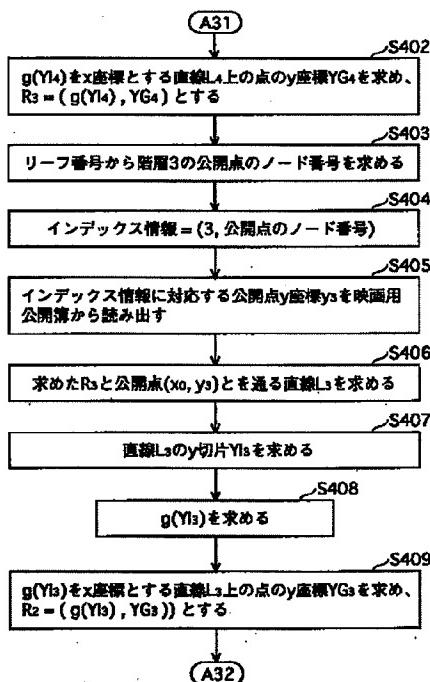
211b

ノード情報				
階層番号	ノード番号	ノード鍵	機器ID	パス情報
1	1	KeyA <sup>(1)</sup>	—	—
2	1	KeyB <sup>(1)</sup>	—	P1
2	2	KeyC <sup>(1)</sup>	—	P2
3	1	KeyD <sup>(1)</sup>	—	P3
3	2	KeyE <sup>(1)</sup>	—	P4
3	3	KeyF <sup>(1)</sup>	—	P5
3	4	KeyG <sup>(1)</sup>	—	P6
4	1	Skdi <sup>(1)</sup>	1001	—
4	2	Skdi <sup>(1)</sup>	1002	—
4	3	Skdi <sup>(1)</sup>	1003	—
4	4	Skdi <sup>(1)</sup>	1004	—
4	5	Skdi <sup>(1)</sup>	1005	—
4	6	Skdi <sup>(1)</sup>	1006	—
4	7	Skdi <sup>(1)</sup>	1007	—
4	8	Skdi <sup>(1)</sup>	1008	—

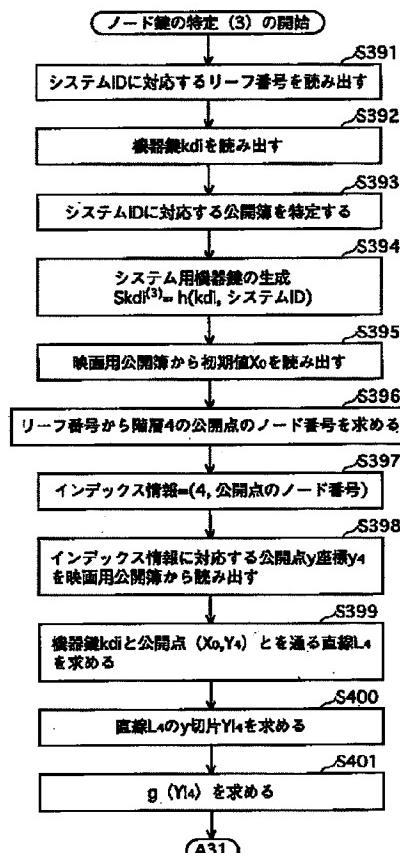
【図37】



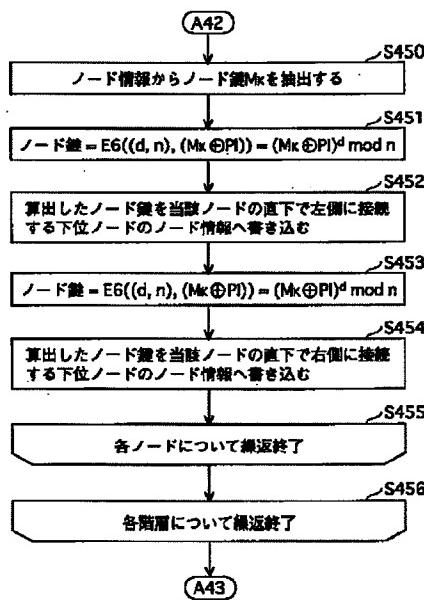
【図42】



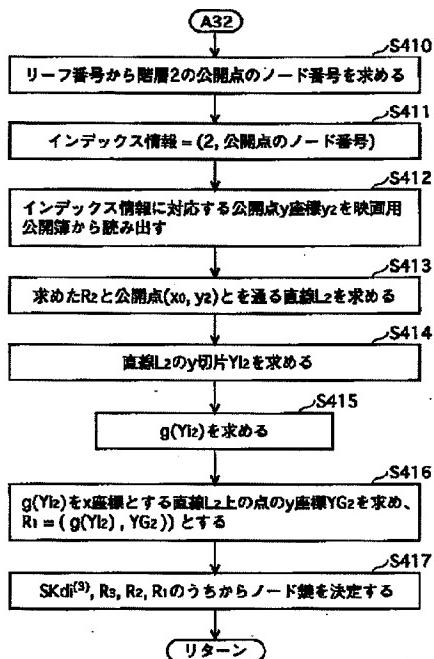
【図41】



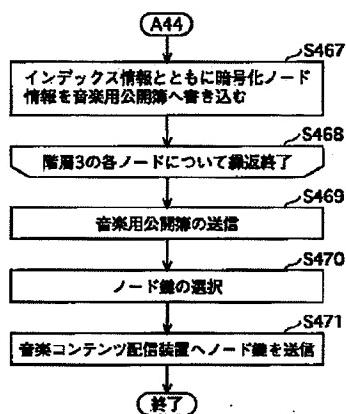
【図49】



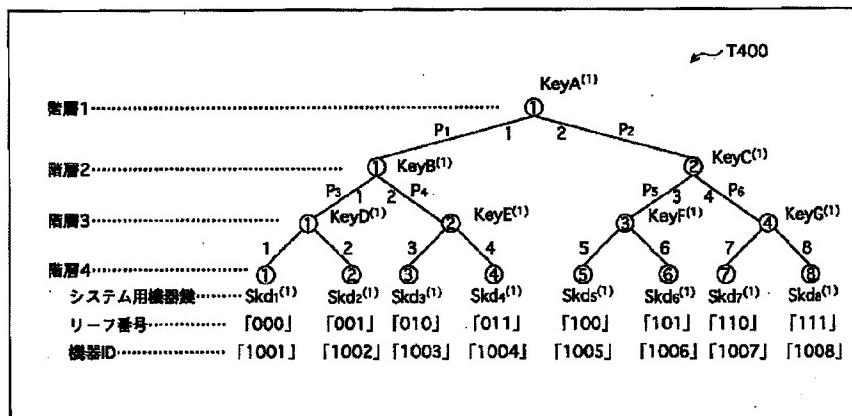
【図43】



【図51】



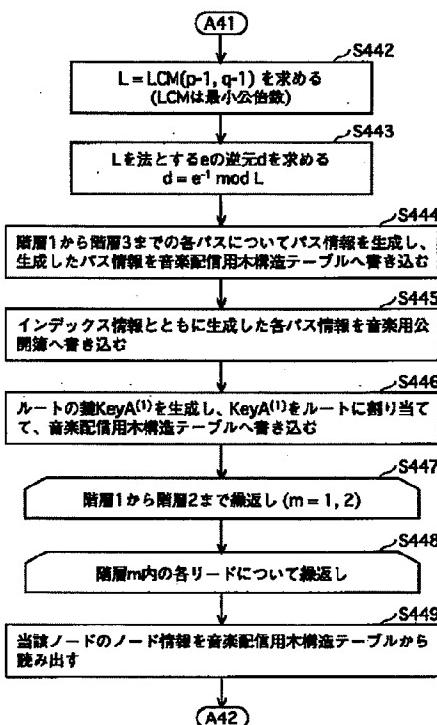
【図44】



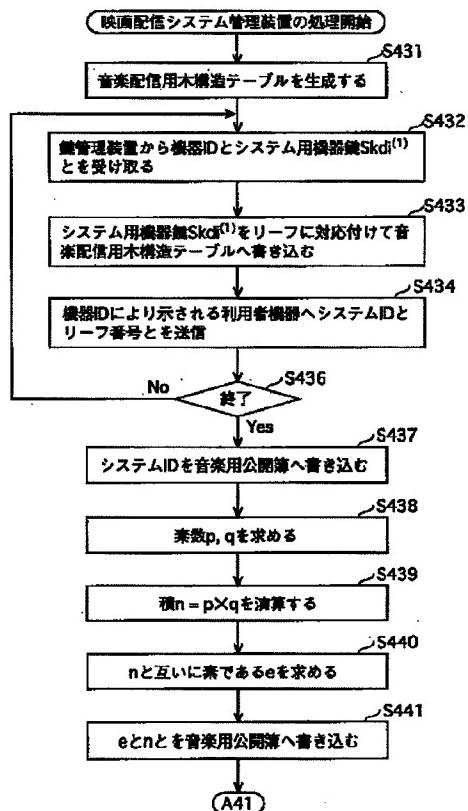
【図46】

音楽用公開簿	
システムID	1
バス公開情報	
公開鍵	e, n
インデックス情報 (階層番号、バス番号)	バス情報
(1, 1)	P <sub>1</sub>
(1, 2)	P <sub>2</sub>
(2, 1)	P <sub>3</sub>
(2, 2)	P <sub>4</sub>
(2, 3)	P <sub>5</sub>
(2, 4)	P <sub>6</sub>
ノード鍵公開情報	
インデックス情報 (階層番号、バス番号)	暗号化ノード鍵
(3, 1)	E <sub>1</sub> (Skd <sub>1</sub> <sup>(1)</sup> , KeyD <sub>1</sub> <sup>(1)</sup> )
(3, 2)	E <sub>1</sub> (Skd <sub>2</sub> <sup>(1)</sup> , KeyD <sub>2</sub> <sup>(1)</sup> )
(3, 3)	E <sub>1</sub> (Skd <sub>3</sub> <sup>(1)</sup> , KeyE <sub>1</sub> <sup>(1)</sup> )
(3, 4)	E <sub>1</sub> (Skd <sub>4</sub> <sup>(1)</sup> , KeyE <sub>2</sub> <sup>(1)</sup> )
(3, 5)	E <sub>1</sub> (Skd <sub>5</sub> <sup>(1)</sup> , KeyF <sub>1</sub> <sup>(1)</sup> )
(3, 6)	E <sub>1</sub> (Skd <sub>6</sub> <sup>(1)</sup> , KeyF <sub>2</sub> <sup>(1)</sup> )
(3, 7)	E <sub>1</sub> (Skd <sub>7</sub> <sup>(1)</sup> , KeyG <sub>1</sub> <sup>(1)</sup> )
(3, 8)	E <sub>1</sub> (Skd <sub>8</sub> <sup>(1)</sup> , KeyG <sub>2</sub> <sup>(1)</sup> )

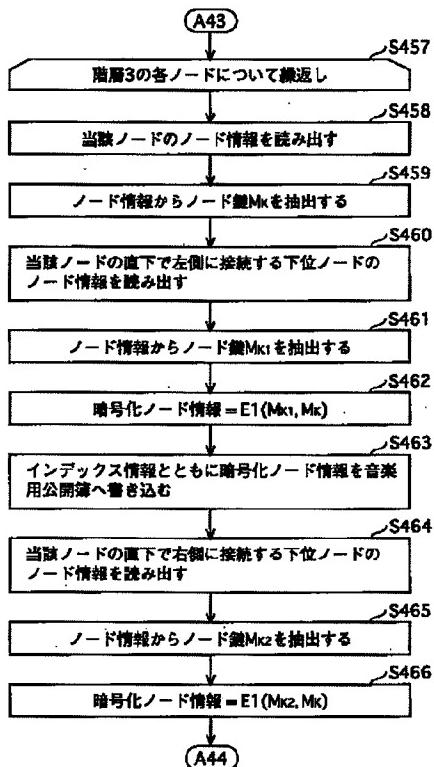
【図48】



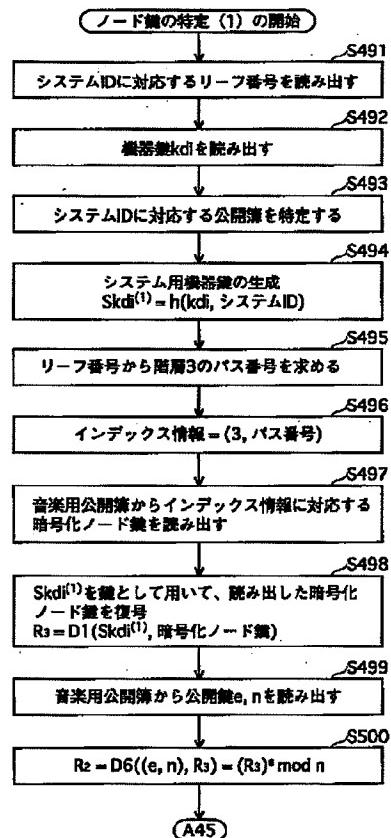
【図47】



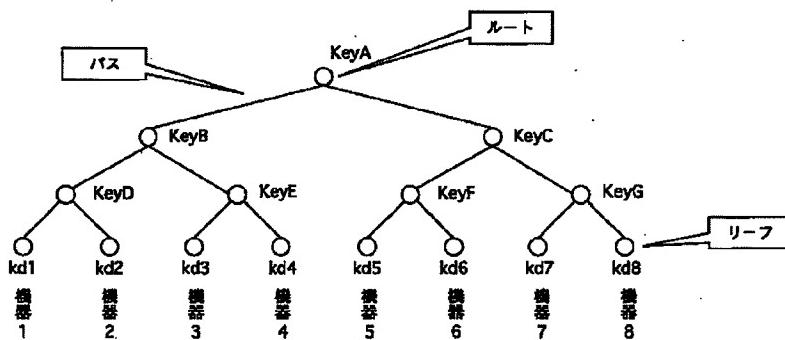
【図50】



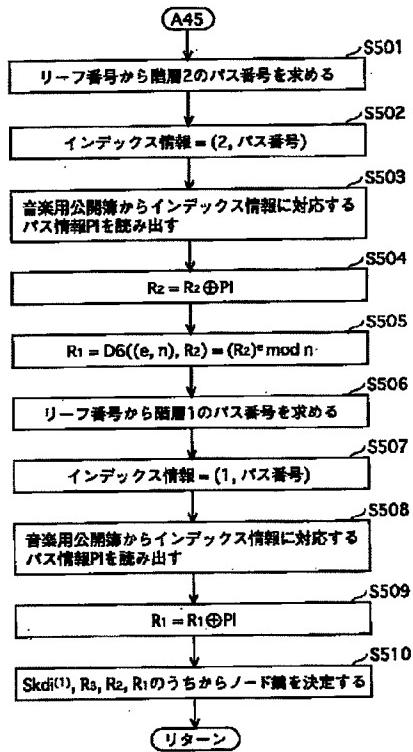
【図52】



【図54】



【図53】




---

フロントページの続き

(72)発明者 松本 勉  
横浜市青葉区柿の木台13-45

F ターム(参考) 5J104 AA12 AA16 EA01 EA04 EA15  
EA19 EA32 JA03 JA21 JA28  
JA31 MA05 NA02 NA11 NA12  
NA18 PA01 PA05 PA14